On subgroups of semi-abelian varieties defined by difference equations

Zoé Chatzidakis[1] (CNRS - Université Paris 7)
Ehud Hrushovski[2] (The Hebrew University of Jerusalem)

Introduction

Consider the algebraic dynamics on an algebraic torus $T = \mathbb{G}_m^n$ given by a matrix $M \in \mathrm{GL}_n(\mathbb{Z})$ Assume no root of unity is an eigenvalue of M. We show that any finite, equivariant map from another algebraic dynamics into (T, M) arises from a group isogeny $\mathbb{G}_m^n \to \mathbb{G}_m^n$. In other words, the automorphism $x \mapsto x^M$ of $K(x) = K(x_1, \ldots, x_n)$ does not extend to any finite field extension, except those contained in $K(x_1^{1/m}, \ldots, x_n^{1/m})$ for some $m \geq 1$. A similar statement is shown for Abelian varieties, and for semi-abelian varieties A.

More generally, we study irreducible difference equations of the form $n\sigma(x) = Mx$, with $M \in \mathrm{End}(A)$, $n \in \mathbb{N}$; for instance the equation $\sigma(x)^3 = x^2$ on $\mathbb{G}_m$. We obtain a similar statement for the function field of such equations.

Model-theoretically, this completes the description ([CH], [CHP], [H]) of the induced structure on ACFA-definable subgroups of semi-Abelian varieties. Such subgroups (up to finite index) are defined by difference equations of the form $n\sigma(x) = Mx$, with $M \in \mathrm{End}(A)$. The induced structure is stable, except when the equation involves the points $A(F)$ of the fixed field or a twisted fixed field $\sigma^r(x) = x^{p^m}$. Whereas the quantifier-free induced structure was understood previously – it corresponds to invariant subvarieties – the full induced structure involves also finite covers, and stability was known only in characteristic zero.

We proceed to describe the result in terms of difference algebra. By a difference field, we mean a field K with a distinguished automorphism σ. The theory ACFA of existentially closed difference fields was extensively studied in [CH] and [CHP]. In these papers, a characterisation of modular types was given, and it was shown that, in characteristic 0, all modular types are stable and stably embedded. In characteristic $p > 0$, we however exhibited examples of modular subgroups of the additive group $\mathbb{G}_a$ which are not stable. The main result of this paper, Theorem (4.6), is that all modular definable subgroups of a semi-abelian variety are stable and stably embedded. This implies that definable subsets of modular subgroups are Boolean combinations of cosets of definable subgroups.

Let F be the transformal function field of a definable subgroup B of a semi-abelian variety A. Stability of B is equivalent to the existence of few difference field extensions L of F, that are finite as field extensions. In fact we obtain a complete description of such extensions. In characteristic zero, the main geometric tool is the ramification divisor of L over appropriate varieties (A or powers of A.) With controlled exceptions, the ramification divisor of a potential extension L is invariant under the dynamics, leading to reduction of the dimension of B. For Abelian varieties, the ramification divisor still carries enough information. If B lives on a torus $\mathbb{G}_m^n$ however, too many finite extensions have the same ramification divisor, and a finer invariant is needed. We consider a certain invariant subspace of the Berkovich space, consisting of valuations with center contained in the

[1] Partially supported by ANR-09-BLAN-0047.
[2] Supported by the Israel Science Foundation 1048/07

ramification divisor. We define an invariant, in the value group, associated with a wildly ramified extension L of F. Within this subspace, there may be no fixed points but there are always recurrent points of the dynamics. Such points lead again to an eigenvector of the dynamics (acting on the value group now) and to a reduction of the dimension of B.

The paper is organised as follows. In section 1 we set up the notation and recall some results on existentially closed difference fields from [C], [CH] and [CHP]. Section 2 recalls the tools used to study definable subgroups of algebraic groups, and describes the criterion for modularity of a definable subgroup of a simple abelian variety or of $\mathbb{G}_m$.

Section 3 contains a host of technical lemmas, which will be used in the proofs of Propositions (4.1) and (4.5). Section 4 contains the proof of Theorem (4.6), and derives some consequences.

1. Notation, preliminary definitions and results

(1.1) **Notation and conventions**. We work in the language $\mathcal{L} = \{+, -, \cdot, 0, 1, \sigma\}$ of difference fields. **All difference fields are inversive**. **Throughout the paper, we work inside a large saturated model** (Ω, σ) **of ACFA**. If K is a difference subfield of Ω, and $A \subset \Omega$, $K(A)_\sigma$ denotes the difference field generated by A over K, and $\mathrm{acl}_\sigma(A)$ the smallest algebraically closed field containing A and closed under σ and σ^{-1}. If A is a subfield of Ω, then A^{alg} denotes the (field-theoretic) algebraic closure of A. We let Frob denote the identity of Ω if the characteristic of Ω is 0, and the automorphism $x \mapsto x^p$ if the characteristic is $p > 0$. If $char(\Omega) = p > 0$ and q is a power of p, we also denote by Frob_q the automorphism $x \mapsto x^q$ of Ω.

If n is a positive integer, we denote by $\mathcal{L}[n]$ the language $\{+, -, \cdot, 0, 1, \sigma^n\}$, viewed as a sublanguage of $\mathcal{L}$, and by $\Omega[n]$ the difference field (Ω, σ^n). Then $\Omega[n]$ is a model of ACFA ([CH], Corollary (1.12)(1)), and is saturated. If E is a difference subfield of Ω, and a a tuple of Ω, then $tp(a/E)[n]$ denotes the type of a over E in the structure $\Omega[n]$.

Recall that the ring of difference polynomials over K in $\bar{X} = (X_1, \ldots, X_n)$, denoted $K[\bar{X}]_\sigma$, is simply the polynomial ring $K[\sigma^j(X_i) \mid i = 1, \ldots, n,\ j \in \mathbb{N}]$. The *$\sigma$-topology on* K^n is the topology with basic closed sets the *σ-closed sets* $\{\bar{a} \in K^n \mid f(\bar{a}) = 0\}$, where $f(\bar{X})$ is a tuple of difference polynomials over K. This topology is Noetherian. When working inside $\Omega[n]$ we will speak of the σ^n-topology.

(1.2) **Some definitions**. Model theoretic algebraic closure coincides with acl_σ ((1.7) in [CH]), and (model-theoretic) independence of algebraically closed sets A and B over a common algebraically closed subset C corresponds to linear independence of the fields A and B over C, and any completion of ACFA is supersimple (see (1.9) in [CH] and use [KP]). We also know that any completion of ACFA eliminates imaginaries ((1.12) in [CH]).

Let E be a difference subfield of Ω, and a a tuple of elements of Ω. Then the quantifier-free type of a over E, denoted $qftp(a/E)$, is the set of quantifier-free $\mathcal{L}$-formulas with parameters in E which are satisfied by a. It therefore describes the isomorphism type of the difference field $E(a)_\sigma$ over E. Similarly, $qftp(a/E)[n]$ denotes the set of quantifier-free $\mathcal{L}[n]$-formulas with parameters in E which are satisfied by a.

The SU-rank is defined as usual. Let us mention that $SU(a/A)$ is finite if and only if $tr.deg(\mathrm{acl}_\sigma(A, a)/\mathrm{acl}_\sigma(A))$ is finite, if and only if all elements of the tuple a satisfy some

non-trivial difference equation over $\mathrm{acl}_\sigma(A)$. We denote by $\mathrm{SU}(a/A)[n]$ the SU-rank in the reduct $\Omega[n]$ (thus it equals $\mathrm{SU}(a/acl_{\sigma^n}(A))[n]$).

Finally, assume that A is a difference subfield of $\Omega[n]$ for some n, and let $a \in \Omega$. We define the eventual SU-rank of a over A, denoted $\mathrm{evSU}(a/A)$, as $lim_{m\to\infty}\mathrm{SU}(a/A)[m!]$ (see (1.13) in [CHP]). It is well-defined, and only depends on $qftp(a/A)$. Note that if $A = \mathrm{acl}_\sigma(A)$ and $\sigma(a) \in A(a)^{alg}$, then $\mathrm{SU}(a/A)[m] \leq \mathrm{SU}(a/A)[mn]$ for all $m, n \neq 0$. This implies that there is some $m > 0$ such that for all $n > 0$, $\mathrm{evSU}(a/A) = \mathrm{SU}(a/A)[mn]$.

(1.3) [bab]**Completions of quantifier-free types**. Let E be a difference subfield of Ω, and a a tuple of elements of Ω. Then $tp(a/E) = tp(b/E)$ if and only if there is an isomorphism $\mathrm{acl}_\sigma(E, a) \to \mathrm{acl}_\sigma(E, b)$, which leaves E fixed and sends a to b ((1.15) in [CH]). In particular, if $E = \mathrm{acl}_\sigma(E)$, then ACFA $\cup qftp(E)$ is complete, and the completions of ACFA are obtained by describing the isomorphism type of the algebraic closure of the prime field.

A *finite σ-stable extension* of a difference subfield K of Ω is a finite (algebraic) extension L of K such that $\sigma(L) = L$. If L is a finite σ-stable extension of K, then so is its normal closure M over K. Furthermore, whether or not $\sigma(M) = M$ does not depend on the extension of σ to M, but is completely determined by the isomorphism type of K: if M is finite Galois over K, let $\alpha \in M$ be such that $M = K(\alpha)$, and let $P(T) \in K[T]$ be the minimal monic polynomial of α over K, and $P^\sigma(T)$ the polynomial obtained by applying σ to the coefficients of P. Then $\sigma(M) = M$ is equivalent to the following statement: the field $K[T]/(P(T))$ contains $\deg(P)$ roots of $P^\sigma(T)$.

Theorem (Babbitt, [C] Theorem 7.VIII). Let E be a difference subfield of Ω, and a, b tuples which have the same quantifier-free type over E. The following conditions are equivalent:
(1) $tp(a/E) = tp(b/E)$.
(2) Given any finite σ-stable Galois extension L of $E(a)_\sigma$, there is an E-embedding $L \to \Omega$ which sends a to b.

In particular, if $E(a)_\sigma$ has no non-trivial finite separable σ-stable extension, then $qftp(a/E)$ is complete.

Let L be a finite σ-stable Galois extension of $E(a)_\sigma$. Then σ induces an automorphism of $G = \mathcal{G}al(L/E(a)_\sigma)$ given by $\rho \mapsto \sigma^{-1}\rho\sigma$; hence, for some ℓ we will have $\sigma^{-\ell}\rho\sigma^\ell = 1$ for all $\rho \in G$.

While it may happen that $E(a)_\sigma$ has some non-trivial finite σ-stable extension, and yet $qftp(a/E)$ be complete, this does not hold if one wants to consider all the reducts $\Omega[n]$. Namely ((2.9)(5) in [CH]):

Lemma. Let F be a difference subfield of Ω. The following conditions are equivalent:
(1) ACFA $\cup\, qftp(F)[n]$ is complete, for all $n > 0$.
(2) F has not finite σ-stable extension.

(1.4) [mod1]**Modularity**. Let $S \subset \Omega^n$ be stable under any $\mathrm{acl}_\sigma(E)$-automorphism of Ω. We say that S is *modular* if whenever a is a tuple of elements of S and $B \subset \Omega$, then a and B are independent over $\mathrm{acl}_\sigma(E, a) \cap acl(E, B)$. A type over E is *modular* if the set of its realisations is modular.

This notion of modularity is also called *one-basedness*. Here we use the fact that our theory is supersimple and eliminates imaginaries. The main result of [CHP] (see (7.5)) shows that S is modular if and only if, for every $F = \mathrm{acl}_\sigma(F)$ containing E and $a \in S$, $tp(a/F)$ is orthogonal to all fixed fields, i.e., to all formulas of the form $\sigma^n(x) = \mathrm{Frob}^m(x)$ where $n \geq 1$, $m \in \mathbb{Z}$. It follows that $tp(a/E)$ is modular if and only $tp(a/E)[\ell]$ is modular for every $\ell \geq 1$, and that a modular type has finite SU-rank.

(1.5) [f1]**Theorem** ([CHP] (7.6)). Let G be an algebraic group and B a definable modular subgroup of $G(\Omega)$. If D is a quantifier-free definable subset of B, then D is a finite Boolean combination of translates of quantifier-free definable subgroups of B. If B is defined over E, then every quantifier-free definable subgroup of B is definable over $\mathrm{acl}_\sigma(E)$.

(1.6) [sse]**Stability and stable embeddability**. A subset S of Ω^m stable under E-automorphisms of Ω is *stably embedded* if whenever $D \subset M^{nm}$ is definable, then $D \cap S^n$ is definable with parameters from S (see the Appendix of [CH] for properties). A type is *stably embedded* if the set of its realisations is stably embedded.

Let $E = \mathrm{acl}_\sigma(E)$, a tuple of elements of Ω. If $tp(a/E)$ is stationary (i.e., has a unique non-forking extension to any set $F \supset E$), then $tp(a/E)$ is definable (this is standard, using compactness). Hence, if all extensions of $tp(a/E)$ to algebraically closed sets are stationary, then $tp(a/E)$ is stable, stably embedded (Lemma 2 in the Appendix of [CH]).

Using the characterisation of modular types and Lemmas 2, 3 of the Appendix of [CH], one easily deduces:

Proposition. Let

$$1 \longrightarrow B_1 \longrightarrow B_2 \longrightarrow B_3 \longrightarrow 1$$

be an exact sequence of groups definable in a model of ACFA. Then B_2 is modular [resp. stable and stably embedded] if and only if B_1 and B_3 are modular [resp. stable and stably embedded].

2. Definable subgroups of algebraic groups

In this chapter we introduce tools used to study definable groups, and give a brief sketch of the description of modular subgroups of abelian varieties. The proof in [H] was given in 0 characteristic, and we indicate what changes need to be made in positive characteristic.

Let G be a connected algebraic group, H a definable subgroup of $G(\Omega)$, everything defined over $E = \mathrm{acl}_\sigma(E) \subset \Omega$.

For each $m \in \mathbb{N}$, define $G_{(m)} = G \times \sigma(G) \times \cdots \times \sigma^m(G)$ and $p_m : G \to G_{(m)}$ by $g \mapsto (g, \sigma(g), \ldots, \sigma^m(g))$. Let $H_{(m)}$ be the Zariski closure of $p_m(H)$, and let $\tilde{H}_{(m)} = \{g \in G \mid p_m(g) \in H_{(m)}\}$. The intersection $\tilde{H}$ of the $\tilde{H}_{(m)}$ equals the σ-closure of H (in $G(K)$), and equals some $\tilde{H}_{(m)}$, because every descending sequence of σ-closed sets stabilises. Then $[\tilde{H} : H] < \infty$: one easily shows that the generics of H (in the model-theoretic sense) are those $h \in H$ such that $p_m(h)$ is a generic of the algebraic group $H_{(m)}$ for every $m > 0$. Hence a generic of H is a generic of $\tilde{H}$.

Because the σ-topology is Noetherian (see [C], 3.V), every σ-closed set S can be expressed as an irredundant union of σ-closed irreducible sets, which are called the irreducible

components of S. Then the irreducible component of $\tilde{H}$ containing the identity of G is a subgroup of $\tilde{H}$; it is called the *connected component of* $\tilde{H}$ and is denoted by $\tilde{H}^0$. Then $[\tilde{H} : \tilde{H}^0] < \infty$. We let $H^0 = H \cap \tilde{H}^0$, and call it the connected component of H. Then also $[H : H^0] < \infty$.

(2.1) **c-minimal subgroups**. Let B be a group definable over K. Then B is *c-minimal* iff every definable subgroup of B is either finite or of finite index in B. Note that c-minimality is preserved by definable homomorphisms with finite kernel; hence if B is c-minimal, then there is a definable homomorphism $g : B_1 \to G(\Omega)$, where B_1 has finite index in B, $\mathrm{Ker}(g)$ is finite central, and G is an algebraic group which is simple as an algebraic group, and which is the Zariski closure of $g(B_1)$.

(2.2) **Definable endomorphisms and subgroups of abelian varieties**. Let A be an abelian variety, defined over $E = \mathrm{acl}_\sigma(E)$. By standard results on abelian varieties, A is isogenous to a finite direct sum of simple abelian varieties defined over E, say to $\bigoplus_{i=1}^n A_i$. Renumbering, we may assume that for $i < j \leq r$, for all $\ell \in \mathbb{Z}$, A_i is not isogenous to $\sigma^\ell(A_j)$, and that for any $j > r$ there are $i \leq r$ and $\ell \in \mathbb{Z}$ such that A_i and $\sigma^\ell(A_j)$ are isogenous. For $i \leq r$ let $m(i)$ be the number of indices j such that for some ℓ, A_i and $\sigma^\ell(A_j)$ are isogenous.

Let us denote by $\mathrm{End}(A)$ the ring of (algebraic) endomorphisms of A, by $\mathrm{Hom}(A, A_i)$ the group of algebraic homomorphisms $A \to A_i$, and by $\mathrm{End}_\sigma(A)$ the ring of definable endomorphisms of $A(\Omega)$, $\mathrm{Hom}_\sigma(A, A_i)$ the group of definable homomorphisms $A \to A_i$. Hrushovski gives a good description of $\mathbb{Q} \otimes \mathrm{End}_\sigma(A)$ in [H], and we refer to this paper for the results quoted below. First, note that $\mathbb{Q} \otimes \mathrm{End}_\sigma(A) \simeq \prod_{i=1}^r M_{m(i)}(\mathbb{Q} \otimes \mathrm{End}_\sigma(A_i))$.

Recall that two definable subgroups B and C of a group are *commensurable* if $B \cap C$ has finite index in both B and C. (One can extend this definition to ∞-definable subgroups by requiring that $B \cap C$ be of bounded index in B and in C). Hrushovski shows that a definable subgroup of $A(\Omega)$ is commensurable to a definable subgroup $\bigcap_{j=1}^n \mathrm{Ker}(F_j)$, where $F_j \in \mathrm{Hom}_\sigma(A, A_j)$.

The study in [H] is made for difference fields of characteristic 0. However, the proofs generalise to positive characteristic without any trouble. Note that in positive characteristic, the Frobenius map may define an endomorphism of the variety.

Theorem 1. Let A be a simple abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, let B be a definable subgroup of $A(\Omega)$.

(1) If there is no integer $n > 0$ such that A and $\sigma^n(A)$ are isogenous, then $\mathrm{End}_\sigma(A) = \mathrm{End}(A)$, and $B = A(\Omega)$.
(2) Assume that there is an integer $n > 0$ such that A and $\sigma^n(A)$ are isogenous. We fix such an n, smallest possible, and choose an isogeny $h : A \to \sigma^n(A)$ of minimal degree m. If $\sigma^n(A) = A$, then we choose h to be the identity. Let $h' : \sigma^n(A) \to A$ be be such that $h'h = [m]$ (multiplication by m in A; such an h' exists by standard results on abelian varieties); then $hh' = [m]$. Define $\tau = \sigma^{-1}h$ and $\tau' = h'\sigma$.

Then $\mathbb{Q} \otimes \mathrm{End}_\sigma(A) \simeq \mathbb{Q} \otimes \mathrm{End}(A)[\tau, \tau']$, and B is commensurable to $\mathrm{Ker}(f)$ for some $f \in \mathrm{End}(A)[\tau, \tau']$. Furthermore, $\mathbb{Q} \otimes \mathrm{End}_\sigma(A)$ is an Ore domain and if $C \subset B$, then C is commensurable to some $\mathrm{Ker}(g)$ with g dividing f (i.e, $hg = f$ for some $h \in \mathbb{Q} \otimes \mathrm{End}_\sigma(A)$).

Proof. In characteristic 0, this is given by Proposition 4.1.1 of [H]. The proof goes through verbatim.

(2.3) **Theorem 2**. Let A be a simple abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let B be a **proper** definable subgroup of $A(\Omega)$, $B = \mathrm{Ker}(f)$, $f \in \mathrm{End}_\sigma(A)$, and assume that f is irreducible in $\mathbb{Q} \otimes \mathrm{End}_\sigma(A)$. Assume that B is not modular.

(1) Then A is isomorphic to an abelian variety A' defined over $\mathrm{Fix}(\rho)$, where $\rho = \mathrm{Frob}^m \sigma^n$ for some $m \in \mathbb{Z}$, $n > 0$.

(2) Assume that A is defined over $\mathrm{Fix}(\theta)$, where $\theta = \mathrm{Frob}^{m'} \sigma^{n'}$ for some $m' \in \mathbb{Z}$, $n' > 0$. If A is not isomorphic to any variety defined over the algebraic closure of the prime field, then f divides $\theta^\ell - 1$ for some ℓ. If A is isomorphic to a variety A' defined over the algebraic closure of the prime field, by an isomorphism F, then for some $m \in \mathbb{Z}$, $n > 0$ and $\rho = \mathrm{Frob}^m \sigma^n$, $F(B) \subset A'(\mathrm{Fix}(\rho))$.

Proof. First observe that the irreducibility assumption on f implies that B is c-minimal.
(1) In characteristic 0, this result is Proposition 4.1.2 of [H]. The proof generalises easily to the positive characteristic case, using the results of [CHP]. Here is a sketch of the main steps: if B is not modular, one knows that the type of a generic of B is non-orthogonal to one of the fixed fields, say $k = \mathrm{Fix}(\rho_0)$, where $\rho_0 = \sigma^n \mathrm{Frob}^m$, $n \geq 1$, and $(n, m) = 1$ if $m \neq 0$. Thus, modulo a finite kernel, it is qf-internal to k, i.e., there is a finite subgroup C of B, and a definable map f from some definable set $S \subset k^\ell$ onto B/C (in fact f is given piecewise by difference rational functions).

Elimination of imaginaries tells us that B/C is then definably isomorphic with a group H_0 living in some cartesian power of k. On the other hand, every subset of a cartesian power of k which is definable in K, is already definable in the difference field k, using maybe extra parameters (see (7.1)(5) in [CHP]). Note that k has SU-rank 1 ((7.1)(1) in [CHP]). An argument similar to the one given in [HP2] or in [KP] then gives us a definable (in k) map $g : H_0' \to H_1(k)$, where $\mathrm{Ker}(g)$ is finite, H_0' is a subgroup of finite index of H_0, and H_1 is an algebraic group defined over k. Then $H_0' \supseteq [n]H_0$ for some n, and because $[H_0 : nH_0] \leq 2n\dim(A)$, we may replace B by $[n]B$, and assume that $H_0' = H_0$.

Composing f and g, we therefore obtain a definable map $h : B \to H_1(k)$, with $\mathrm{Ker}(h)$ finite. We may assume that the Zariski closure of $h(B)$ is all of H_1.

Since B is c-minimal, so is $h(B)$, and this implies that if $\pi : H_1 \to A'$ is a projection of H_1 onto a simple quotient A' of H_1, then $\pi h(B)$ is Zariski dense in A', and therefore $\mathrm{Ker}\pi \cap h(B)$ is finite. Replacing ρ_0 by some power $\rho = \rho_0^r$ (and k by its algebraic extension of degree r), we may assume that A' and π are defined over k. Hence we get a definable map $B \to A'(k)$, with finite kernel. This implies that $\mathrm{Hom}(A, \sigma^\ell(A')) \neq (0)$ for some ℓ, and applying some power of σ to A', we may assume that $\mathrm{Hom}(A, A') \neq 0$. Thus A' is a simple abelian variety, defined over k, and isogenous to A. This implies that A is isomorphic to an abelian variety A'' defined over some finite extension of k. Replacing ρ by its appropriate power, we have shown (1).

(2) By (1), we have a definable map $\varphi : B \to A'(k)$, with finite kernel D, where $\rho = \mathrm{Frob}^m \sigma^n$ and $k = \mathrm{Fix}(\rho)$. Moreover A' is isogenous to A. If $mn' = m'n$, then we may assume that $\theta = \rho$ and $A' = A$. If $mn' \neq m'n$, then A is isomorphic to a variety A'' defined over $\mathrm{Fix}(\theta)^{alg} \cap \mathrm{Fix}(\rho)^{alg} = \mathbb{F}_p^{alg}$, and we are in the second case. The result will follow from the following claim:

Claim. Let A be an abelian variety defined over $k = \mathrm{Fix}(\rho)$, let B be a definable subgroup of $A(\Omega)$ and $\varphi : B \to A(k)$ a definable homomorphism with finite kernel D. Then $B \subseteq A(\mathrm{Fix}(\rho^\ell))$ for some ℓ.

Proof. The graph of φ is a definable subgroup of A^2; as there are only countably many of those (see 4.1.10 in [H]), it must be defined over k^{alg}. Hence, φ is definable over k^{alg}, and, replacing ρ by an appropriate power we may assume that φ is defined over $\mathrm{Fix}(\rho)$. Let $k_0 \prec k$ be such that everything is defined over k_0. Since D is finite, if $b \in B$ then $b \in \mathrm{acl}_\sigma(k_0(\varphi(b))) = k_0(\varphi(b))^{alg}_\sigma$. By compactness, there is ℓ such that $[k_0(\varphi(b))_\sigma(b) : k_0(\varphi(b))_\sigma] \leq \ell$ for every $b \in B$ and this implies that $b \in \mathrm{Fix}(\rho^{\ell!})$.

(2.4) **Definable subgroups of tori**. Similar results hold for tori, i.e., algebraic groups isomorphic to $\mathbb{G}_m^n$ for some n. Namely, $\mathbb{Q} \otimes \mathrm{End}_\sigma(\mathbb{G}_m)$ is isomorphic to $\mathbb{Q}[\sigma, \sigma^{-1}]$, and definable subgroups of $\mathbb{G}_m$ are commensurable to subgroups of the form $\mathrm{Ker}(f)$, for $f \in \mathbb{Z}[\sigma, \sigma^{-1}]$ (note that σ acts trivially on $\mathbb{Z}$, so that $\mathbb{Q} \otimes \mathrm{End}_\sigma(\mathbb{G}_m)$ is in fact the ring of Laurent polynomials in σ). Moreover, $\mathbb{Q} \otimes \mathrm{End}_\sigma(\mathbb{G}_m^n) \simeq M_n(\mathbb{Q}[\sigma, \sigma^{-1}])$. Modular subgroups of $\mathbb{G}_m$ are those which are commensurable to some $\mathrm{Ker}(f)$, where f is relatively prime to all elements of the form $\sigma^k - p^m$, with $k > 0$ and $m \in \mathbb{Z}$.

3. Technical lemmas

In this chapter we collect some technical lemmas which will be used in the proof of the main results.

(3.1) [alg1]**Conventions and some basic results and definitions in algebraic geometry**. Recall that we work in a large saturated model (Ω, σ) of ACFA. Our varieties will always be quasi-projective and absolutely irreducible. The function field of the variety V will be denoted by $\Omega(V)$, and viewed as a set of rational functions on V. If $x \in V$, then $\mathcal{O}_{x,V}$ will denote the ring of functions of $\Omega(V)$ which are defined at x, and $\mathcal{M}_{x,V}$ its maximal ideal, which consists of functions vanishing at x.

A dominant morphism $f : V \to W$ induces a dual morphism $f^* : \Omega(W) \to \Omega(V)$. A morphism $f : V \to W$ between two varieties is finite if for every $x \in V$, $\mathcal{O}_{x,V}$ is integral algebraic over $f^*\mathcal{O}_{f(x),W}$. The dominant finite morphism f is *unramified over* y) if for every $x \in f^{-1}(y)$, $\mathcal{O}_{x,V}/\mathcal{M}_{y,W}\mathcal{O}_{x,V}$ is a field which is separably algebraic over $\mathcal{O}_{y,W}/\mathcal{M}_{y,W}$ (using the natural inclusion induced by f^*). If W is normal, this is equivalent to saying that $f^{-1}(y)$ contains $deg(f)$ distinct points, where $deg(f) = [\Omega(V) : f^*\Omega(W)]$. The locus of ramification of f is the set of points of W over which f is ramified. This is a closed subset of W. If $f : V \to W$ is finite unramified and flat, then f is *étale*.

If $f : V \to W$ is finite unramified over $f(x)$, then f induces an isomorphism between the tangent spaces $T_x(V)$ and $T_{f(x)}(W)$.

(3.2) [su1]**Lemma**. Let $E = \mathrm{acl}_\sigma(E)$, let B be a definable modular subgroup of some algebraic group G defined over E, and let a be a generic of B. Assume that $\sigma(a) \in E(a)^{alg}$, and for $\ell \geq 0$ let V_ℓ be the algebraic locus of $(a, \sigma(a), \ldots, \sigma^\ell(a))$ over E. Assume that for some $\ell > 0$, the variety V_ℓ has a proper infinite subvariety W such that $\pi_0(W)^{\sigma^\ell} = \pi_\ell(W)$ have the same dimension as W, where $\pi_0 : V_\ell \to V_0$ and $\pi_\ell : V_\ell \to V_0^{\sigma^\ell}$ are the natural projections given by the inclusion $V_\ell \subset V_0 \times V_0^\sigma \times \cdots \times V_0^{\sigma^\ell}$. Then $\mathrm{evSU}(a/E) > 1$.

Proof. Tranlating a by some element of B, we may assume that $B = B^0$, i.e., that each V_ℓ is a group. The assumption $\sigma(a) \in E(a)^{alg}$ implies that all varieties V_ℓ have the same dimension as V_0, and that $\dim(W) < \dim(V_0)$. Consider the projection $(\pi_0 \times \pi_\ell) : V_\ell \to V_0 \times V_0^{\sigma^\ell}$. Then $(\pi_0 \times \pi_\ell)(W)$ is a proper subvariety of $(\pi_0 \times \pi_\ell)(V_\ell)$. The set $B(\ell) = \{x \in \Omega \mid (x, \sigma^\ell(x)) \in (\pi_0 \times \pi_\ell)(V_\ell)\}$ is a σ^ℓ-closed subgroup of $G(\Omega)$, containing the σ^ℓ-closure of B as a subgroup of finite index. Therefore $B(\ell)$ is modular, of the same evSU-rank as B. By (1.11), the subset $\{x \in G(\Omega) \mid (x, \sigma^\ell(x)) \in (\pi_0 \times \pi_\ell)(W)\}$ is a Boolean combination of cosets of quantifier-free definable subgroups of $B(\ell)$, and in fact, is a finite union of such cosets. As $0 < \dim(W) < \dim(V_0)$, this implies that $B(\ell)$ contains some definable subgroup C which is infinite and of infinite index in $B(\ell)$. Thus $\mathrm{SU}(a/E)[\ell] > 1$ because a is a generic of B.

(3.3) [ram1]**Lemma**. Let $E = \mathrm{acl}_\sigma(E)$, U a non-singular variety defined over E, $f : W \to U$ the normalisation of U in some finite separable extension of $E(U)$. Let s, g be finite morphisms such that $\mathrm{Frob}_q : U^{1/q} \to U$ factors as $\mathrm{Frob}_q = gs$, with $s : U^{1/q} \to U'$, $g : U' \to U$, and U' non-singular, and let (W_1, f_1) be the normalisation of U' in $E(U')(W)$ (Here, $U^{1/q}$ denotes $U^{\mathrm{Frob}_q^{-1}}$). If f ramifies over $u \in U$, then f_1 ramifies over $g^{-1}(u)$.

Proof. The fields $E(W)$ and $E(U^{1/q})$ are linearly disjoint over $E(U)$. Hence, if W' is an irreducible component of $W \times_U U'$ projecting onto U, then the map $f' : W' \to U'$ is finite separable. Hence we have a birational map $t : W_1 \to W'$ such that $f't = f_1$, and (W_1, t) is the normalisation of W'.

Consider the finite morphism $j : W^{1/q} \to W \times U'$ defined by $j(w) = (w^q, sf^{1/q}(w))$; then $j(W^{1/q}) \subset W \times_U U'$, and therefore $j(W^{1/q}) = W'$. Because $W^{1/q}$ is normal, the one-to-one morphism j factors through W_1. Hence, if f ramifies over $x \in U$, then f_1 ramifies over $g^{-1}(x)$.

(3.4) [ram0b]**Lemma**. Let $E = \mathrm{acl}_\sigma(E)$, and a such that $a \in E(\sigma(a))^s$, $\mathrm{evSU}(a/E) = 1$, and a belongs to a definable modular subgroup of some abelian algebraic group G defined over E.

Let U be the closed projective variety over E of which a is a generic, and let $V \subset U \times U^\sigma$ be the locus of $(a, \sigma(a))$, π_0, π_1 the natural morphisms $V \to U$ and $V \to U^\sigma$.

Let X_0 be the closed subset of U defined by

$$\begin{aligned} X_0 =& \mathrm{Sing}(U) \cup \pi_0\pi_1^{-1}(\mathrm{Sing}(U^\sigma)) \cup \\ & \{x \in U \mid |\pi_0^{-1}(x)| \neq |\pi_0^{-1}(a)|\} \cup \{x \in U \mid |\pi_1^{-1}(\sigma(x))| \neq |\pi_1^{-1}(\sigma(a))|\}, \end{aligned}$$

where $\mathrm{Sing}(U)$ denotes the singular locus of U, and let $U_0 = U \setminus X_0$. Let X be the smallest subset of U containing X_0 and satisfying $\pi_0^{-1}(X) = \pi_1^{-1}(X^\sigma) = Y$. Then X is a countable union of closed subsets of U.

If $\sigma(a) \notin E(a)^s$, then we assume that $\dim(U) \geq 2$, and that the map π_0 on $V_0 = \pi_0^{-1}(U_0) \cap V$ factors as $\pi_0 = hg$, where h, g are finite, h is unramified, and for some power q of p, if $U_1 = g(V_0)$ then U_1 is non-singular and there is a finite morphism s on ${U_1}^{1/q}$ such that $gs = \mathrm{Frob}_q$.

Let L be a finite Galois extension of $E(a)$ which is linearly disjoint from $E(a)_\sigma$ over $E(a)$, and is such that $L(\sigma(a)) = \sigma(L)(a)$. We let $f : W_0 \to U_0$ be the normalisation of U_0 in L.

Then the ramification divisor of f (on U_0) is contained in X.

Proof. Assume that this is not the case, and let $\mathcal{S}$ be the set of irreducible components of the ramification divisor of f which are not contained in X. Then $\mathcal{S}$ is finite, and $\mathcal{S}^\sigma$ is the analogous set for $f^\sigma : W_0^\sigma \to U_0^\sigma$.

Note that because U_0 is non-singular and f is finite, all components of the ramification divisor of f have co-dimension 1 in U_0. Note also that all points of V_0 are non-singular points of $U \times U^\sigma$. Hence if $D \subset U_0$ is irreducible, then all components of $\pi_0^{-1}(D)$ will project onto D: this follows from the dimension theorem applied to $V_0 \cap (D \times U^\sigma)$, and the fact that the map π_0 is finite on V_0.

We will show the following:

Claim. If $D \in \mathcal{S}$ and D' is any irreducible component of $\pi_0^{-1}(D)$, then $\pi_1(D') \in \mathcal{S}^\sigma$.

Let us first assume that π_0 is separable. Because $E(a)_\sigma$ and L are linearly disjoint over $E(a)$, the set $W_0 \times_{U_0} V_0$ has a unique irreducible component W_1 projecting onto U. By assumption, the map $\pi_0 : V_0 \to U_0$ is finite unramified, and hence the map $\pi_0' : W_1 \to W_0$ induced by $W_1 \subseteq W_0 \times V_0 \to W_0$ is finite unramified. Note that both these maps are étale, and that W_1 is normal. This implies that if $f_1 : W_1 \to V_0$ is the map induced by $W_1 \subset (W_0 \times V_0)$, and $v \in V_0$, then f_1 is ramified over v if and only if f is ramified over $\pi_0(v)$. Hence, if D_1 is a subvariety of V_0 of codimension 1, then D_1 is contained in the ramification divisor of f_1 if and only if $\pi_0(D_1) \in \mathcal{S}$.

Similarly, $W_0^\sigma \times_{U_0^\sigma} V$ has a unique irreducible component W_2 which projects onto U_0^σ, and W_2 is normal (because π_1 is étale on $\pi^{-1}(U_0^\sigma)$). If D_2 is a subvariety of $\pi_1^{-1}(U_0^\sigma)$ of codimension 1, then D_2 is contained in the ramification divisor of $f_2 : W_2 \to V$ if and only if $\pi_1(D_2) \in \mathcal{S}^\sigma$.

Because $L(\sigma(a)) = \sigma(L)(a)$, there is a birational map $\varphi : W_1 \to W_2$ which induces the identity on V. Consider now $T_1 = W_1 \cap (W_0 \times \pi_1^{-1}(U_0^\sigma))$ and $T_2 = W_2 \cap (W_0^\sigma \times V_0)$. They both project (by finite morphisms) onto $T_0 = V_0 \cap \pi_1^{-1}(U_0^\sigma)$, and are normal; hence T_1 is the normalisation of T_0 in M, and so is T_2. Because φ induces the identity on T_0, it follows that φ is an isomorphism between T_1 and T_2. In particular, because $f_1 = f_2\varphi$, if $D_1 \subset T_0$ is a component of the ramification divisor of $f_1|_{T_1}$ it is also a component of the ramification divisor of $f_2|_{T_2}$.

Putting everything together shows the claim in the case where π_0 is separable, because T_0 projects onto a subset of U containing $U \backslash X$. Let us now assume that π_0 is not separable. We need to show that if $f_1 : W_1 \to V_0$ is the normalisation of V_0 in $L(\sigma(a))$, and $D \in \mathcal{S}$, then all components of $\pi_0^{-1}(D)$ are in the ramification divisor of f_1. The rest of the proof is as in the previous case.

We have $U_1 = g(V_0)$. Reasoning as above, the irreducible component W' of $W_0 \times_{U_0} U_1$ projecting onto U_0 is normal, and if $f' : W' \to U_1$ is the map induced by $W_0 \times U_1 \to U_1$, then (W', f') is the normalisation of U_1 in $LE(U_1)$. Furthermore, if $D \in \mathcal{S}$, then $h^{-1}(D)$ is contained in the ramification divisor of f'. By Lemma (3.3), $g^{-1}h^{-1}(D)$ is contained in the ramification divisor of f_1. But $g^{-1}h^{-1} = (hg)^{-1} = \pi_0^{-1}$.

This finishes the proof of the claim. Let us first assume that $\dim(U) \geq 2$. For each $k > 0$, let V_k be the complete subvariety of $(U \times U^\sigma \times \cdots \times U^{\sigma^k})$ locus of $(a, \ldots, \sigma^k(a))$ over E. The hypotheses on X imply that the singular locus of V_k is contained in $X_k =$

$X \times X^\sigma \times \cdots \times X^{\sigma^k}$. Moreover, for every finite non-empty $J \subset \{0, 1, \ldots, k\}$, the natural projection $\pi_{J,k} : V_k \to \prod_{j \in I} U^{\sigma^j}$ is finite outside of X_k. This implies that irreducible subvarieties of V_k not contained in X_k are sent by $\pi_{J,k}$ to irreducible subvarieties of the same dimension, and that they lift to subvarieties of V_{k+1} of the same dimension. Thus, for each k, if $D_0 \in \mathcal{S}$, then there is a subvariety D' of V_k which projects onto D_0 (via the map $\pi_{\{0\},k}$), and we then have that $D_i = \pi_{\{i\},k}(D') \in \mathcal{S}^{\sigma^i}$. If k is $\geq |\mathcal{S}|$, there are indices $0 \leq i < j \leq k$ such that $\sigma^{-i}(D_i) = \sigma^{-j}(D_j)$. Then $\dim(D_i) = \dim(U) - 1 > 0$, and Lemma (3.2) applies and gives us the desired contradiction.

Let us now assume that $\dim(U) = 1$. Then both maps π_0 and π_1 are finite unramified on $\pi_0^{-1}(U_0)$ and $\pi_1^{-1}(U_0^\sigma)$ respectively. Each member of $\mathcal{S}$ corresponds to a discrete valuation v on $E(a)$ which ramifies in L. Let us denote this set of discrete valuations by $\mathcal{V}$. Note that our hypothesis on X implies that the elements of $\mathcal{V}$ do not ramify in any subextension of $E(a)_\sigma$. The assertion $\pi_0^{-1}(\mathcal{S}) = \pi_1^{-1}(\mathcal{S}^\sigma)$ then translates to: if $v \in \mathcal{V}$, and w is a valuation on $E(a, \sigma(a))$ extending w, then the restriction of w to $E(\sigma(a))$ is in $\mathcal{V}^\sigma$, and if w' is a valuation on $E(a, \sigma^{-1}(a))$ extending v, the restriction of w' to $E(\sigma^{-1}(a))$ is in $\mathcal{V}^{\sigma^{-1}}$. From this one deduces by induction that for every $k \in \mathbb{Z}$, if w is a valuation on $E(a, \sigma^k(a))$ which extends v, then the restriction of w to $E(\sigma^k(a))$ is in $\mathcal{V}^{\sigma^k}$.

On the other hand, because $tp(a/E)$ is modular and $tr.deg(a/E) = 1$, we know that the set $\{[E(a, \sigma^k(a)) : E(a)]_s \mid k \in \mathbb{Z}\}$ is unbounded (see (4.5) in [CH]). Here, the separable degree $[E(a, \sigma^k(a)) : E(a)]_s$ equals $[E(a, \sigma^k(a)) : E(a)]$ by assumption. Choose $k \in \mathbb{Z}$ such that $[E(a, \sigma^k(a)) : E(a)] = N > |\mathcal{S}|$. Because v is unramified in $E(a, \sigma^k(a))$, v has N distinct extensions to $E(a, \sigma^k(a))$, and these extensions restrict to N distinct valuations on $E(\sigma^k(a))$ which are in $\mathcal{V}^{\sigma^k}$. This gives the desired contradiction.

(3.5) [ram2]**Remark**. The only place where we used the hypothesis that a is the generic of a modular definable group, is in Lemma (3.2), to be able to deduce that $\mathrm{evSU}(a/E) > 1$. In the general case of an element a of evSU-rank 1 over E, the proof of (3.4) only shows that the ramification divisor of f on U must be defined over E.

(3.6) [lem1] **Lemma**. Let G be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let B be a definable subgroup of $G(\Omega)$ of finite SU-rank. Let $n \in \mathbb{N}$, and let a be a generic of B over E, and b such that $[n]b = a$. Then $E(b)_\sigma$ is a finite σ-stable (Galois) extension of $E(a)_\sigma$.

Proof. We use the notation introduced at the beginning of section 2. The truth of this statement only depends on $qftp(a/E)$ (see (2.9)(2) in [CH]), and we may therefore assume that $b \in B$, and that $B = \tilde{B}$. Since $[B : B^0]$ is finite, we may also assume that $B = B^0$. Let m be such that $B = \tilde{B}_{(m)}$, and let $N \geq m$. Then $B_{(N)}$ is a semi-abelian variety which projects onto $B_{(m)}$ with finite fibers, so that $|B_{(N)}[n]| = |B_{(m)}[n]| \leq n^{2\dim(B_{(m)})}$. Then $(b, \sigma(b), \ldots, \sigma^N(b))$ is a generic of $B_{(N)}$, and $\mathcal{G}al(E(b, \sigma(b), \ldots, \sigma^N(b))/E(a, \ldots, \sigma^N(a))$ is isomorphic to a subgroup of $B_{(N)}[n]$. This implies that for every $N \geq m$,

$$[E(b, \sigma(b), \ldots, \sigma^N(b))/E(a, \ldots, \sigma^N(a))] \leq |B_{(N)}[n]| = |B_{(m)}[n]|$$

whence $[E(b)_\sigma : E(a)_\sigma]$ is finite.

(3.7) [lem31]**Lemma**. Let $E = \mathrm{acl}_\sigma(E) \subseteq F = \mathrm{acl}_\sigma(F)$, and let a be independent from F over E. Assume that L is a proper finite σ-stable extension of $\mathrm{acl}_\sigma(Ea)F$. Then there is F_1, independent from (a, F) over E, and a finite σ-stable extension M of $FF_1(a)_\sigma$ such that $L \subset \mathrm{acl}_\sigma(F_1 a)M$.

Proof. $\mathrm{acl}_\sigma(Ea)F$ is a Galois extension of $F(a)_\sigma$, and the Galois closure of L over $F(a)_\sigma$ is therefore a finite σ-stable extension of $\mathrm{acl}_\sigma(Ea)F$ (see (2.9)(3) in [CH]); we may therefore assume that L is Galois over $F(a)_\sigma$. Recall that we work inside the large difference field Ω. Let φ be an $\mathrm{acl}_\sigma(Ea)$-automorphism of Ω such that $\varphi(F) = F_1$ is independent from (F, a) over E, and let $L_1 = \varphi(L)$. Then LL_1 is a Galois extension of $FF_1(a)_\sigma$, which contains $\mathrm{acl}_\sigma(Ea)F$, and we will identify

$$\mathcal{G}al(LL_1/FF_1(a)_\sigma) \simeq \mathcal{G}al(L/F(a)_\sigma) \times_{\mathcal{G}al(\mathrm{acl}_\sigma(Ea)/E(a)_\sigma)} \mathcal{G}al(L_1/F_1(a)_\sigma).$$

Consider the subgroup H of $\mathcal{G}al(LL_1/FF_1(a)_\sigma)$ defined by

$$H = \{(\tau, \varphi\tau\varphi^{-1}) \mid \tau \in \mathcal{G}al(L/F(a)_\sigma)\}.$$

As φ is an $\mathrm{acl}_\sigma(Ea)$-isomorphism of difference fields, H is a subgroup of $\mathcal{G}al(LL_1/FF_1(a)_\sigma)$, which projects onto $\mathcal{G}al(\mathrm{acl}_\sigma(Ea)/E(a)_\sigma)$ and $\sigma^{-1}H\sigma = H$. Observe that $[\mathcal{G}al(LL_1/FF_1(a)_\sigma) : H] = [L : \mathrm{acl}_\sigma(Ea)F]$ is finite. Hence, the subfield M of LL_1 which is fixed by H is a finite σ-stable extension of $FF_1(a)_\sigma$, and intersects $\mathrm{acl}_\sigma(Ea)FF_1$ in $FF_1(a)_\sigma$.

We have $\mathcal{G}al(LL_1/L_1) \cap H = (1)$, whence $L_1M = LL_1$. From $L_1 \subset \mathrm{acl}_\sigma(F_1 a)$, we obtain the result.

(3.8) **Lemma**. [lem4] Let $E = \mathrm{acl}_\sigma(E)$, a a finite tuple, and assume that M is a finite σ-stable Galois extension of $E(a)_\sigma$. Then there is $n \in \mathbb{N}$ and a finite Galois extension L of $E(a, \ldots, \sigma^n(a))$ such that $M = LE(a)_\sigma$, $[L : E(a, \ldots, \sigma^n(a))] = [M : E(a)_\sigma]$ and $\sigma(L)(a) = L(\sigma^{n+1}(a))$.

Proof. Fix α generating M over $E(a)_\sigma$. Then there are integers $i \leq j$ such that the extension $M_0 = E(\sigma^i(a), \ldots, \sigma^j(a), \alpha)$ of $E(\sigma^i(a), \ldots, \sigma^j(a))$ is Galois, of degree $[M : E(a)_\sigma]$. By assumption, $\sigma(M_0) \subseteq M_0E(a)_\sigma$ and $M_0 \subseteq \sigma(M_0)E(a)_\sigma$. Hence there are integers $\ell \leq i$ and $k \geq j$ such that $\sigma(M_0) \subseteq M_0E(\sigma^\ell(a), \ldots, \sigma^k(a))$ and $M_0 \subseteq \sigma(M_0)E(\sigma^\ell(a), \ldots, \sigma^k(a))$. Define $L = \sigma^{-\ell}(M_0)E(a, \ldots, \sigma^{-\ell+k}(a))$. Then L is Galois over $E(a, \ldots, \sigma^{-\ell+k}(a))$, of degree $[M : E(a)_\sigma]$. An easy computation shows that $\sigma(L) \subseteq L(\sigma^{-\ell+k+1}(a))$ and $L \subseteq \sigma(L)(a)$.

(3.9) [lem5]. Let $E = \mathrm{acl}_\sigma(E)$, a a finite tuple such that $\sigma(a) \in E(a)^{alg}$. Assume that L is a finite Galois extension of $E(a)$, which is linearly disjoint from $E(a)_\sigma$ over $E(a)$ and is such that $L(\sigma(a)) = \sigma(L)(a)$.

(1) Let $n \geq 1$, $m \in \mathbb{Z}$ and $\tau = \sigma^n\mathrm{Frob}^m$. Let $b = (a, \sigma(a), \ldots, \sigma^{n-1}(a))$ and $L' = L(b)$. Then $L'(\tau(b)) = \tau(L')(b)$.

(2) Let $n = tr.deg(a/E)$. There is $m \in \mathbb{Z}$ such that if $\tau = \sigma^n\mathrm{Frob}^m$ and $b = (a, \sigma(a), \ldots, \sigma^{n-1}(a))$, then $b \in E(\tau(b))^s$. If $n = 1$, then also $\tau(a) \in E(a)^s$.

Proof. (1) As $E(b)_\tau \subset E(a)_\sigma^{1/p^\infty}$, $L(b)$ and $E(b)_\tau$ are linearly disjoint over $E(b)$. Let α be a generator of L over $E(a)$. Then $\sigma^n(\alpha) = \tau(\alpha)^{p^{-m}} \in E(b, \sigma^n(a), \alpha) \subset E(b, \sigma^n(b), \alpha)$.

Assume $m > 0$. Then $\tau(\alpha)$ generates a Galois extension of $E(\tau(a))$, and belongs to $E(b, \sigma^n(b), \alpha)$. But $E(b, \sigma^n(b))$ is a purely inseparable extension of $E(b, \tau(b))$, and therefore $\tau(\alpha) \in E(b, \tau(b), \alpha)$. The linear disjointness of L' and $E(b)_\tau$ over $E(b)$ implies then that $E(b, \tau(b), \alpha) = E(b, \tau(b), \tau(\alpha))$. The case $m < 0$ is done in a similar fashion.

(2) We know that $b \in E(\sigma^n(b))^{alg}$, and we choose $m \leq 0$ such that $b \in E(\sigma^n(b)^{p^m})^s$. This shows the first part.

Assume now that $tr.deg(a/E) = 1$. Choose an element c of a such that $E(a) \subset E(c)^s$, and let $f(X, Y) \in E[X, Y]$ be the irreducible polynomial satisfied by $(c, \sigma(c))$. Then $f(X, Y)$ is separable in one of the variables X, Y, and without loss of generality it is separable in X. Write $f(X, Y) = g(X, Y^{p^m})$ where $g(X, Y)$ is separable in Y (and in X), and let $\tau = \sigma \mathrm{Frob}^m$. Then $g(c, \tau(c)) = 0$, so that $E(c)_\tau \subset E(c)^s$. Since $a \in E(c)^s$, we obtain $E(a)_\tau \subset E(c)^s$.

(3.10) [val1]**Generalised power series**. Recall that if Γ is an ordered abelian group and E a field, then the field of generalised power series $E((t^\Gamma))$ is defined as the set of all formal sums $f = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ with $a_\gamma \in E$ and such that $\mathrm{Supp}(f) = \{\gamma \in \Gamma \mid a_\gamma \neq 0\}$ is well-ordered.

We define a valuation v on $E((t^\Gamma))$ by $v(f) = \inf \mathrm{Supp}(f)$, and a coefficient map $\mathrm{co} : E((t^\Gamma)) \to E$ by $\mathrm{co}(f) =$ coefficient of $t^{v(f)}$ in f, i.e., the unique element $a \in E$ such that $v(f - at^{v(f)}) > v(f)$. If $a \in E((t^\Gamma))$ and $\gamma \in \Gamma$, we denote by $a_{|\gamma}$ the unique element b of $E((t^\Gamma))$ with support contained in $(-\infty, \gamma]$ and such that $v(a - b) > \gamma$.

We denote by $E[t^\Gamma]$, [resp. $E(t^\Gamma)$] the subring [resp. subfield] of $E((t^\Gamma))$ generated by E and all elements t^γ, $\gamma \in \Gamma$. The following result is probably well-known, but for lack of a reference we will give its proof.

(3.11) [val2]**Proposition**. Let E be a field, and Γ an ordered subgroup of $\mathbb{R}$, such that $\bigcap_{n \in \mathbb{N}} p^n \Gamma = (0)$ if $char(E) = p > 0$. The elements of $E((t^\Gamma))$ which are separably algebraic over $E(t^\Gamma)$ have the following property: their support is either finite or of order type ω and cofinal in $\mathbb{R}$. The subring $E[t^\Gamma] = E[t^\gamma \mid \gamma \in \Gamma]$ is dense in $E(t^\Gamma)^s \cap E((t^\Gamma))$.

Proof. We consider the completion $E(t^\Gamma)^c$ of $E(t^\Gamma)$ with respect to the valuation. This is the smallest field containing limits of all sequences $(a_n)_{n \in \mathbb{N}}$ of elements of $E(t^\Gamma)$, with $v(a_{n+1} - a_n)$ increasing and cofinal in $\mathbb{R}$. Then $E(t^\Gamma)^c$ is henselian (see Chapter 2 of [S]).
Claim. $E(t^\Gamma)^c$ coincides with the set R of elements of $E((t^\Gamma))$ whose support is either finite or of order type ω and cofinal in Γ.

Note that $a \in R$ if and only if for every $\gamma \in \mathbb{R}$, $\mathrm{Supp}(a) \cap (-\infty, \gamma)$ is finite. Clearly R contains $E[t^\Gamma]$ and is closed under addition. For multiplication, let $a, b \in R$, $\gamma \in \mathbb{R}$; then $\mathrm{Supp}(ab) \cap (-\infty, \gamma) \subset \mathrm{Supp}(a_{|\gamma - v(b)} \cdot b_{|\gamma - v(a)})$. Similarly, if $a \in R$ with $v(a) > 0$, $\gamma > 0$, and k is the smallest integer such that $kv(a) > \gamma$, then $\mathrm{Supp}((1+a)^{-1}) \cap (-\infty, \gamma) \subset \mathrm{Supp}(1 + a_{|\gamma} + \cdots + a^{k-1}{}_{|\gamma})$. This implies that R is a subfield of $E((t^\Gamma))$. It follows that every element of $E(t^\Gamma)^c$ is the limit of a sequence of elements of $E[t^\Gamma]$, and therefore coincides with R.

Thus the ring $E[t^\Gamma]$ is dense in $E(t^\Gamma)^c$: for every $a \in E(t^\Gamma)^c$ and $\gamma \in \mathbb{R}$, there is $b \in E[t^\Gamma]$ such that $v(a - b) > \gamma$.

The field $E(t^\Gamma)^c$ is henselian, and if $char(E) = 0$, it is has no proper immediate algebraic extension, so that the result holds. Assume now that $char(E) = p > 0$, and

that L is a finite Galois extension of $E(t^\Gamma)^c$. We need to show that $L \cap E((t^\Gamma)) \subset E(t^\Gamma)^c$. Suppose that this is not the case, and let e be the prime-to-p divisor of the ramification index of v in L, and $\Gamma' = (1/e)\Gamma$. Then $LE^s(t^{\Gamma'})^c$ is a Galois extension of $E^s(t^{\Gamma'})^c$ of degree a power of p, and is contained in $E^s((t^{\Gamma'}))$. If L is not contained in $E^s(t^{\Gamma'})^c$, then there is $a \in L$ such that $b = a^p - a \in E^s(t^{\Gamma'})^c$, $a \notin E^s(t^{\Gamma'})^c$. Write $b = \sum_{i=0}^m b_i t^{\gamma_i} + c$, where $b_i \in E^s$, $\gamma_0 < \gamma_1 < \cdots < \gamma_m < 0$ and $v(c) \geq 0$. We claim that there is $d \in E^s[t^{\Gamma'}]$ such that $d^p - d = \sum_{i=0}^m b_i t^{\gamma_i}$. Otherwise, replacing each $b_i t^{\gamma_i}$ by $b_i^{1/p^k} t^{\gamma_i/p^k}$ where k is largest such that p^k divides γ_i and $b_i^{1/p^k} \in E^s$, we may assume that either p does not divide γ_0, or $b_0^{1/p} \notin E^s$, and this leads to a contradiction, as in $E^{alg}((t^{\mathbb{R}}))$ we have $v(a - b_0^{1/p} t^{\gamma_0/p}) > v(a)$, so that $E^s(t^{\Gamma'})^c(a)$ would not be an immediate extension of $E^s(t^{\Gamma'})^c$.

Thus there is $d \in E^s[t^{\Gamma'}]$ such that $v(b - d^p + d) \geq 0$. Since $E^s(t^{\Gamma'})^c$ is henselian, $a \in E(t^{\Gamma'})^c$.

We have shown that $L \cap E^s((t^{\Gamma'})) \subset E^s(t^{\Gamma'})^c$. As $E^s(t^{\Gamma'})^c \cap E((t^\Gamma)) = E(t^\Gamma)^c$, this proves the result.

(3.12) [val3]**Algebraically closed valued fields**. Consider the theory of algebraically closed valued fields in the 2-sorted language (K, Γ, v), where v is the valuation map : $K \to \Gamma \cup \{\infty\}$, and K and Γ are structures in the languages $\{+, -, \cdot, 0, 1\}$ and $\{+, -, 0, \leq\}$ respectively. V. Weispfenning [W] showed that this theory eliminates quantifiers. (Other quantifier elimination results for algebraically closed valued fields were obtained by A. Robinson [R] and F. Delon [D].)

Let (K, v) be an algebraically closed valued field, E an algebraically closed subfield on which v is trivial, and assume that $\bar{a} = (a_1, \ldots, a_n) \in K$ is such that $v(a_1), \ldots, v(a_n)$ are $\mathbb{Q}$-linearly independent. Quantifier elimination then implies that $tp(a_1, \ldots, a_n/E)$ is completely determined by $tp(v(a_1), \ldots, v(a_n))$ (in Γ), i.e., by the set of formulas $\sum_{i=1}^n m_i \xi_i > 0$ (where $m_i \in \mathbb{Z}$) satisfied by $v(\bar{a}) = (v(a_1), \ldots, v(a_n))$.

Let $\alpha \in E(a_1, \ldots, a_n)^s$. Then $v(\alpha)$ belongs to the $\mathbb{Q}$-vector space generated by $v(a_1), \ldots, v(a_n)$; thus there are $\mathbb{Q}$-linear combinations $t_1(\bar{\xi}), \ldots, t_k(\bar{\xi})$ such that the values of the conjugates of α over $E(a_1, \ldots, a_n)^s$ are in the set $\{t_1(v(\bar{a})), \ldots, t_k(v(\bar{a}))\}$. Let $P(\bar{a}, X)$ be the minimal polynomial of α over $E(\bar{a})$. Since $tp(v(\bar{a})) \vdash tp(\bar{a}/E)$, there is a finite conjunction $\psi(\bar{\xi})$ of formulas of the form $\sum_{i=1}^n m_i \xi_i > 0$ such that if $\bar{b} \in K$ is such that $v(\bar{b})$ satisfies ψ, and if β is a root of $P(\bar{b}, X)$, then $v(\beta) \in \{t_1(v(\bar{b})), \ldots, t_k(v(\bar{b}))\}$.

(3.13) [val4]**Algebraically closed valued fields of rank** 1. Let E be an algebraically closed field of characteristic $p > 0$, and consider the (algebraically closed) valued field $(E((t^{\mathbb{R}})), v)$. We fix a positive integer n and define $\mathcal{R}$ to be the set of n-tuples of $\mathbb{R}^n$ which are $\mathbb{Q}$-linearly independent.

Let $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathcal{R}$, and let $\Gamma = \langle \gamma \rangle$ be the subgroup of $\mathbb{R}$ generated by the elements of γ. Let $\bar{a} = (t^{\gamma_1}, \ldots, t^{\gamma_n})$, let $F = E(\bar{a})$, and $\alpha \in F^s \cap E((t^\Gamma))$, $P(\bar{a}, X)$ its minimal polynomial over F.

By Proposition (3.11), there is some $Q(\bar{a}) \in E[\bar{a}, \bar{a}^{-1}]$ such that

$$v(P(Q(\bar{a})) = v(\alpha - Q(\bar{a})) > \sup\{0, 2v(P'(\bar{a}, \alpha))\}.$$

This is an elementary statement, and so there is a definable set D containing γ such that if $\delta = (\delta_1, \ldots, \delta_n) \in D$, $\bar{b} = (t^{\delta_1}, \ldots, t^{\delta_n})$, then $P(\bar{b}, X)$ has a root β satisfying

$v(P(Q(\bar{b})) = v(\beta - Q(\bar{b})) > \sup\{0, 2v(P'(\bar{b}, \beta))\}$. Note that by Hensel's lemma, the condition $v(P(Q(\bar{b}))) > 2v(P'(\bar{b}, \beta))$ will imply that this β is in $E((t^{\langle\delta\rangle}))$. Furthermore, assume that the field generated over $F(\alpha)$ by a root of the equation $X^p - X = \alpha$ is a ramified extension of F. This means that the element $R(\bar{a}) = \alpha_{|0}$ is not of the form $h^p - h$ in the ring $E[\bar{a}, \bar{a}^{-1}]$. If δ is sufficiently close to γ, we will have $\beta_{|0} = R(\bar{b})$. If $\delta \in \mathcal{R}$, this will then imply that the field generated over $E(\bar{b}, \beta)$ by a root of $X^p - X - \beta$ is ramified over $E(\bar{b}, \beta)$.

Because $\gamma \in \mathcal{R}$, any definable set containing γ will contain an open ball $B(\gamma; \varepsilon) = \{\delta \in \mathbb{R}^n \mid \|\delta - \gamma\| < \varepsilon\}$ for some $\varepsilon > 0$ (here $\| \ \|$ denotes the usual norm in Euclidean space).

(3.14) [val5]**Lemma**. Let $A \in GL_n(\mathbb{Q})$, with $n > 1$. Suppose that for every $m \geq 1$, the characteristic polynomial of A^m is irreducible over $\mathbb{Q}$. Let $S \subset \mathcal{R}$ with the following properties:

— $A(S) \subset S \neq \emptyset$,

— if $0 \neq r \in \mathbb{R}$, then $rS = S$.

— S is closed in $\mathcal{R}$.

Then there is $\gamma \in S$ such that for every $\varepsilon > 0$, there are infinitely many integers m such that

$$\Big\| \frac{A^m(\gamma)}{\|A^m(\gamma)\|} - \frac{\gamma}{\|\gamma\|} \Big\| < \varepsilon.$$

Proof. Our assumption on A implies that for every $m \geq 1$, $\mathbb{R}^n$ has no A^m-stable subspace defined over $\mathbb{Q}$ (other than (0), $\mathbb{R}^n$). This implies that if V is a proper subspace of $\mathbb{R}^n$ defined over $\mathbb{Q}$, then V cannot contain a subspace $W \neq (0)$ which is A^m-stable for some $m \geq 1$: otherwise $\bigcap_n A^{mn}(V)$ would be a proper subspace of $\mathbb{R}^n$ containing W and defined over $\mathbb{Q}$. It also implies that all eigenvalues of A^m are distinct and non-zero.

We will work in $\mathbb{P}^{n-1}(\mathbb{R})$, and we denote by $\tilde{S}$, $\tilde{\mathcal{R}}$, the images of S and $\mathcal{R}$ in $\mathbb{P}^{n-1}(\mathbb{R})$. Let T be the closure of $\tilde{S}$ in $\mathbb{P}^{n-1}(\mathbb{R})$; then T is compact and A-invariant. We call a point c of $\mathbb{P}^{n-1}(\mathbb{R})$ *recurrent* if for every open set U containing c the set $\{m \in \mathbb{N} \mid A^m(c) \in U\}$ is infinite.

Since S is closed in $\mathcal{R}$, it suffices to show that T contains a recurrent point which is in $\tilde{\mathcal{R}}$, since this point will necessarily be in $\tilde{S}$.

Take a maximal chain of non-empty closed A-invariant subsets of T; then the intersection C of this chain is non-empty and is minimal closed A-invariant. Thus if $c \in C$ and $k \geq 1$, then c belongs to the adherence of $\{A^m(c) \mid m \geq k\}$, so that c is recurrent. Note also that $A(C) = C$.

Assume that $C \cap \tilde{\mathcal{R}}$ is empty. Thus C is covered by a union of hyperplanes of $\mathbb{P}^{n-1}(\mathbb{R})$ which are defined over $\mathbb{Q}$. By Baire's lemma, there is an open subset O of $\mathbb{P}^{n-1}(\mathbb{R})$ and a hyperplane H defined over $\mathbb{Q}$ such that $C \cap O \subset H$. Note that $\bigcup_{m\in\mathbb{Z}} A^m(O)$ is an open set which is A-invariant and intersects C; by minimality of C, it contains C, and by compactness, there is a finite subset I of $\mathbb{Z}$ such that $C = \bigcup_{m\in I} A^m(C \cap O)$. Hence $C \subset \bigcup_{m\in I} A^m(H)$. From $A(C) = C$, we deduce that $\bigcap_{n\in\mathbb{N}} A^n(\bigcup_{m\in I} A^m(H))$ is non-empty and A-invariant. I.e, there are subspaces $V_1, \ldots, V_r$ defined over $\mathbb{Q}$ of $\mathbb{P}^{n-1}(\mathbb{R})$ such

that $C \subset V_1 \cup \cdots \cup V_r = A(V_1 \cup \cdots \cup V_r)$. Thus A permutes the spaces V_i, and $A^{r!}(V_i) = V_i$ for any i. This contradicts our assumption.

4. The main result.

(4.1) [ram3b] **Proposition**. Let A be an abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, let B be a definable modular subgroup of $A(\Omega)$, with $\mathrm{evSU}(B) = 1$, let a be a generic of B over E, and let M be a finite σ-stable Galois extension of $E(a)_\sigma$. Then for some N and b satisfying $[N]b = a$, $M \subset E(b)_\sigma$.

Proof. Replacing a by $(a, \ldots, \sigma^{n-1}(a))$ for some n, we may assume that $\sigma(a) \in E(a)^{alg}$, and that $M = LE(a)_\sigma$, where L is finite Galois over $E(a)$, linearly disjoint from $E(a)_\sigma$ over $E(a)$, and such that $L(\sigma(a)) = \sigma(L)(a)$ (see Lemma (3.8)). By (3.9), we may also assume that $a \in E(\sigma(a))^s$, and if $tr.deg(a/E) = 1$, that $\sigma(a) \in E(a)^s$.

Let U and V be the abelian varieties which are the loci of a and of $(a, \sigma(a))$ respectively over E. Let $f : W \to U$ be the normalisation of U in L. We will show that $W \to U$ is unramified.

The variety V is contained in $U \times U^\sigma$, projects onto U and U^σ via the projections π_0, π_1, which are isogenies. Since $a \in E(\sigma(a))^s$, the map π_1 is étale. We wish to show that the hypotheses of Lemma (3.4) are satisfied. The map π_0 may not be separable, but it is an isogeny. Hence it factors as $\pi_0 = hg$, where h is an étale isogeny, and g is purely inseparable. If $U_1 = g(U)$, then U_1 is an abelian variety, and if $q = deg(g)$, then the isogeny $\mathrm{Frob}_q : U_1^{1/q} \to U_1$ factors through V. Hence the hypotheses of Lemma (3.4) are satisfied, with $X = \emptyset$, and therefore $f : W \to U$ is unramified. By a result of Lang-Serre [LS], this implies that W is isomorphic over E to an abelian variety A', and that f is a translate of an isogeny $A' \to A$. As E is algebraically closed, this implies that $L \subset E(b)$ where $[N]b = a$ for some $N > 0$.

(4.2) [ram4]**Lemma**. Let B be a modular subgroup of $\mathbb{G}_m(\Omega)$, let a be a generic of B over $E = \mathrm{acl}_\sigma(E)$, and assume that $\mathrm{evSU}(B) = 1$, and $tr.deg(E(a)_\sigma/E) = n$, and $a \in E(\sigma(a), \ldots, \sigma^n(a))^s$. Assume that L is a finite Galois extension of $E(a, \ldots, \sigma^{n-1}(a))$ such that $\sigma(L)(a) = L(\sigma(a))$ and L is linearly disjoint from $E(a)_\sigma$ over $E(a, \ldots, \sigma^{n-1}(a))$. Let (W, f) be the normalisation of $\mathbb{G}_m^n$ in L. Then f is unramified over all points of $\mathbb{G}_m^n$.

Proof. The element a satisfies an equation of the form $\prod_{i=0}^n \sigma^i(a^{m_i}) = 1$, where the m_i's are in $\mathbb{Z}$, with no common divisor, and p does not divide m_0. Let q be the highest power of p dividing m_n, let $e = m_n/q$, and $V \subset \mathbb{G}_m^{n+1}$ the subgroup defined by $\prod_{i=0}^n \sigma^i(a^{m_i}) = 1$.

Let $g(x_0, \ldots, x_n) = (x_0, \ldots, x_{n-1}, x_n^q)$, $h(x_0, \ldots, x_n) = (x_0, \ldots, x_{n-1})$. Then $\pi_0 = hg$ and $g(\mathbb{G}_m^{n+1}) = U_1$ is the subgroup of $\mathbb{G}_m^{n+1}$ defined by the equation $x_n^e \prod_{i=0}^{n-1} x_i^{m_i} = 1$, so that the map h is étale on U_1. Furthermore, the map $\mathrm{Frob}_q : {U_1}^{1/q} \to U_1$ factors through V, by the map $s : (x_0, \ldots, x_n) \mapsto (x_0^q, \ldots, x_{n-1}^q, x_n)$. Thus Lemma (3.4) applies if $n > 1$.

If $n = 1$, then replace σ by $\tau = \sigma\mathrm{Frob}_q$. Then $a^{m_0}\tau(a)^e = 1$. By Lemma (3.9) and Lemma (3.3), we get the result.

(4.3) While we will not use this result here, let us mention the analogous fact for $\mathbb{G}_a$:

Lemma. Let B be a modular subgroup of $\mathbb{G}_a(\Omega)$ of evSU-rank 1, defined over $E = \mathrm{acl}_\sigma(E)$, and let $a \in B$, $a \notin E$. Assume that $a \in E(\sigma(a), \ldots, \sigma^n(a))^s$. Let L be a finite Galois

extension of $E(a,\dots,\sigma^{n-1}(a))$ such that $\sigma(L)(a) = L(\sigma^n(a))$ and L is linearly disjoint from $E(a)_\sigma$ over $E(a,\dots,\sigma^{n-1}(a))$. Let $U \subset \mathbb{G}_a^n$ be the algebraic locus of $(a,\dots,\sigma^{n-1}(a))$ over E, and let (W,f) be the normalisation of U in L. Then f is unramified over all points of U.

Proof. Because B is a subgroup of $\mathbb{G}_a$, the minimal polynomial of $\sigma^n(a)$ over $E(a,\dots,\sigma^{n-1}(a))$ is of the form $F_n(X) + \sum_{i=0}^{n-1} F_i(\sigma^i(a)) = 0$, where each F_i is an additive polynomial over E. By assumption, F_0 is separable, because $F_0(X) + \sum_{i=1}^{n} F_i(\sigma^i(a)) = 0$ is the minimal polynomial of a over $E(\sigma(a),\dots,\sigma^n(a))$. Write $F_n(X) = F(X^q)$ where $F(X)$ is additive separable, and let $\bar{x} = (x_0,\dots,x_{n-1})$, $\bar{y} = (y_0,\dots,y_{n-1})$. Then V is the subgroup of $\mathbb{G}_a^{2n}$ defined by $\bar{x} \in U$, $x_{i+1} = y_i$ for $i = 0,\dots,n-2$, and $F_n(y_{n-1}) + \sum_{i=0}^{n-1} F_i(x_i) = 0$, and U and V are non-singular. If $q \neq 1$, then the map π_0 factors as hg, where $g(\bar{x},\bar{y}) = (\bar{x}, y_{n-1}^q)$, and $h(x_0,\dots,x_{n-1},y) = (x_0,\dots,x_{n-1})$. Moreover $V_1 = g(V)$ is the subgroup of $\mathbb{G}_a^{n+1}$ defined by $\bar{x} \in U$, $\sum_{i=0}^{n-1} F_i(x_i) + F(y) = 0$, so that $h : V_1 \to U$ is étale, and $\mathrm{Frob}_q : V_1^{1/q} \to V_1$ factors through V via the map $(\bar{x},y) \mapsto (\bar{x}^q, y)$.

Again, if $n = 1$, then by Lemma (3.9) we may replace σ by $\tau = \sigma\mathrm{Frob}^\ell$ for some ℓ and therefore assume that $F(X) = F_n(X)$. Thus Lemma (3.4) applies and gives that f is unramified.

(4.4) Before plunging into the proof in the toric case, we describe it in a simplified setting. Using the additive notation, the subgroups in question can be written:

$$B = \{x \in \mathbb{G}_m^n \mid \sigma(x) = Mx\},$$

where $M \in \mathrm{GL}_n(\mathbb{Q})$ (denominators should be cleared in the obvious way). We treat here the case $M \in \mathrm{GL}_n(\mathbb{Z})$; a slight extension will work for $M \in \mathrm{GL}_n(\mathbb{Z}_p) \cap \mathrm{GL}_n(\mathbb{Q})$, but the general case is harder. In addition, we describe here for simplicity only Galois extensions L of the function field $E(B)$ of order p. We show that if any such L exists, then $\mathbb{G}_m(\mathrm{Fix}(\sigma))$ is involved in B.

For any valuation v of $E(B)$, if $L = E(B)(x)$ with $x^p - x = c \in E(B)$, and $v(c) < 0$ and $v(c)$ is not divisible by p, then it is easy to see that $v(c)$ is uniquely determined; any c' with the same conditions will have $v(c') = v(c)$. In fact, $c(1+\mathcal{O}_v)$ is similarly determined. We let $\theta(L,v) = v(c)$ for any such c.

Any group embedding of $\mathbb{Z}^n = \mathrm{Hom}(\mathbb{G}_m^n, \mathbb{G}_m)$ into $\mathbb{R}$ induces a Berkovich point, i.e. an $\mathbb{R}$-valued valuation on $E(B)$ over E. Let X be the space of all such valuations. The automorphism σ of $E(B)$ induces an automorphism σ of X. We may have no fixed point but we find a recurrent point v of this action (projectively, i.e. up to equivalence of valuations). Let G be the value group of v, a subgroup of $\mathbb{R}$. Then $\sigma^m(v) = v \circ \sigma^{-m}$ is a valuation with value group G; we have a group automorphism of G, still denoted σ, satisfying $v(\sigma(x)) = \sigma(v(x))$.

Of course, σ does not preserve the ordering on G. But it does preserve (non)divisibility by p. Moreover since v was chosen recurrent, for any given element b of $E(B)$, for infinitely many k, b is negative for v iff it is negative for $\sigma^k(v)$. It follows that $\theta(L,v) = \theta(L,\sigma^k(v))$ for infinitely many k.

However, this means that some σ^k has a fixed vector in its action on G. Thus the characteristic polynomial of M is not irreducible, and indeed $\mathbb{G}_m(\mathrm{Fix}(\sigma))$ is non-orthogonal to B. This finishes the sketch of proof in this easy case.

(4.5) [prop1]**Proposition**. Let B be a definable modular subgroup of $\mathbb{G}_m(\Omega)$ of evSU-rank 1 and which is connected for the σ-topology. Let $E = \mathrm{acl}_\sigma(E)$, let a be a generic of B over E, and assume that M is a finite σ-stable Galois extension of $E(a)_\sigma$. Then $M \subseteq E(a^{1/N})_\sigma$ for some N.

Proof. Let $n = tr.deg(E(a)_\sigma/E)$; then a satisfies an equation $\prod_{i=0}^n \sigma^i(x^{d_i}) = 1$, where the d_i's are integers. Since B is connected, the d_i's have no common divisor. By Lemma (3.9) (applied to σ^{-1}), we may also assume that p does not divide d_n, and if $n = 1$, that in addition p does not divide d_0.

Since the existence of such an M only depends on $qftp(a/E)$, we may also assume that for every $m > 1$, a has an m-th root in B. Replacing a by $a^{1/m}$ for some m, this will allow us to assume that for any $N > 1$, the extensions M and $E(a^{1/N})_\sigma$ are linearly disjoint over $E(a)_\sigma$.

We define an action of σ on $\mathbb{Q}^n$ and on $\mathbb{R}^n$ by $\sigma(\gamma) = A\gamma$ where

$$A = \begin{pmatrix} 0 & 0 & \dots & -d_0/d_n \\ 1 & 0 & \cdots & -d_1/d_n \\ 0 & 1 & \cdots & -d_2/d_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -d_{n-1}/d_n \end{pmatrix}.$$

Then $f(T) = \sum_{i=0}^n d_i T^i$ is the characteristic polynomial of A. Since $\mathrm{evSU}(B) = 1$, $f(T)$ is irreducible over $\mathbb{Q}$, and so is the characteristic polynomial of A^m for any $m \geq 1$. Hence $\mathbb{Q}^n$ has no proper σ^m-stable subspace for any $m \geq 1$. Moreover, by modularity of B, $f(T)$ is relatively prime to all polynomials of the form $T^m - p^\ell$ where $m \geq 1$, $\ell \in \mathbb{Z}$.

Observe also that if v is an E-valuation on $E(a)_\sigma$ such that $\gamma = (v(a), \dots, v(\sigma^{n-1}(a))) \in \mathbb{R}^n$ and $\ell > 0$, then $A^\ell\gamma = (v(\sigma^\ell(a)), \dots, v(\sigma^{\ell+n-1}(a)))$.

Step 1. We may assume that conjugation by σ induces the identity on $\mathcal{G}al(M/E(a)_\sigma)$.

There is some ℓ such that σ^ℓ commutes with the elements of $\mathcal{G}al(M/E(a)_\sigma)$. Since $\mathbb{Q}^n$ has no proper σ^ℓ-stable subspace, this implies that $\sigma(a), \dots, \sigma^{n-1}(a)$ belong to the $\mathbb{Q}$-subspace of $\mathbb{Q}^n$ generated by $a, \sigma^\ell(a), \dots, \sigma^{\ell(n-1)}(a)$; hence, for some $N \geq 1$ they belong to the group generated by $a^{1/N}, \sigma^\ell(a^{1/N}), \dots, \sigma^\ell(a^{1/N})$. We replace a by $a^{1/N}$, and σ by σ^ℓ.

Step 2. We may assume that $M = LE(a)_\sigma$, where L is finite Galois over $E(a, \dots, \sigma^{n-1}(a))$, linearly disjoint from $E(a)_\sigma$ over $E(a, \dots, \sigma^{n-1}(a))$, and satisfies $L(\sigma^n(a)) = \sigma(L)(a)$.

By Lemma (3.8), there is some $m \geq n$ such that the desired conclusion holds with m replacing n. Note that $\sigma^n(a) \in E(a^{1/d_n}, \dots, \sigma^{n-1}(a)^{1/d_n})$. Let $N = d_n^{m-n}$: the assumption that $M \cap E(a^{1/N})_\sigma = E(a)_\sigma$ implies that by replacing a by $a^{1/N}$ and L by $L(a^{1/N}, \dots, \sigma^{n-1}(a^{1/N}))$, we obtain the desired conclusion.

Step 3. If e is prime to p and is such that $[L : E(a, \dots, \sigma^{n-1}(a))]/e$ is a power of p, then we may assume that L is defined over $E(a^e, \dots, \sigma^{n-1}(a^e))$, i.e., that $L = L'(a, \dots, \sigma^{n-1}(a))$ for some finite σ-stable Galois extension L' of $E(a^e, \dots, \sigma^{n-1}(a^e))$.

We just replace a by $a^{1/e}$, and L by $L(a^{1/e}, \dots, \sigma^{n-1}(a^{1/e}))$.

Step 4. Consider the set $\mathcal{V}$ of E-valuations v on $E(a,\dots,\sigma^{n-1}(a))$ such that $v(a) = \gamma_0,\dots,v(\sigma^{n-1}(a)) = \gamma_{n-1}$ are $\mathbb{Q}$-linearly independent, and v ramifies in L. Then $\mathcal{V}$ is non-empty.

Let i be such that if $F = E(a,\dots,\sigma^{i-1}(a),\sigma^{i+1}(a),\dots,\sigma^n(a))$ then $L \not\subset F^{alg}(\sigma^i(a))$. Because the projective line has no proper étale cover, there is an F-valuation w on $F(\sigma^i(a))$ with value group isomorphic to $\mathbb{Z}$ and which ramifies in L. By (4.2) (applied to σ^{-1}), we know that $w(\sigma^i(a)) = \pm 1$: otherwise there is some irreducible polynomial $P(T) \in F[T]$ not equal to T, such that $w(P(\sigma^i(a))) = 1$; this polynomial then yields a hypersurface of $\mathbb{G}_a^n$ over which f ramifies, and which is not contained in $\mathbb{G}_m^n$, contradicting (4.2).

Let Δ be an ordered group generated by elements $\gamma_0,\dots,\gamma_{n-1}$ which are $\mathbb{Q}$-linearly independent, and let $\Gamma = \mathbb{Z} \oplus \Delta$ with the lexicographical ordering. Define an E-valuation v on $F(\sigma^i(a))$ by setting $v(\sigma^j(a)) = (0,\gamma_j)$ if $j \neq i$, and $v(\sigma^i(a)) = (1,0)$. Then v ramifies in L because w does.

Step 5. The set of valuations $v \in \mathcal{V}$ with value group contained in $\mathbb{R}$ is non-empty.

Let us write $\bar{a} = (a,\dots,\sigma^{n-1}(a))$. Extend the valuation v of Step 4 to a valuation on some algebraically closed field K containing $E(\bar{a})$, and let $u \in L$ be such that $v(u) = \sum_{j=0}^{n-1} m_j v(\sigma^j(a)) \notin v(E(\bar{a}))$ (the m_j's are in $\mathbb{Q}$); let $P(\bar{a},T) \in E[\bar{a},T]$ the minimal polynomial of u over $E(\bar{a})$. Then, in the valued field (K,v), $tp(\bar{a}/E) \vdash \exists y P(\bar{x},y) = 0 \wedge v(y) = \sum_j m_j v(x_j)$.

By elimination of quantifiers of the theory of algebraically closed fields, and because the elements of $v(\bar{a})$ are $\mathbb{Q}$-linearly independent (see the discussion in (3.12)), there is a formula $\psi(\bar{\xi})$ satisfied by the n-tuple $v(\bar{a})$, which is a conjunction of formulas of the form $\sum_{j=0}^{n-1} m_j \xi_j > 0$, and such that whenever $\bar{b} = (b_0,\dots,b_{n-1})$ is any n-tuple in (K,v), such that $v(\bar{b})$ satisfies ψ, then some root u' of $P(\bar{b},T) = 0$ has valuation $\sum_j m_j v(b_j)$. Choose some n-tuple $\delta = (\delta_0,\dots,\delta_{n-1}) \in \mathcal{R}$ satisfying ψ, and define the E-valuation v_δ on $E(\bar{a})$ by setting $v_\delta(a_j) = \delta_j$. Then $v_\delta \in \mathcal{V}$ has value group contained in $\mathbb{R}$.

Step 6. Definition of $S \subset \mathcal{R}$.

Let $\gamma \in \mathcal{R}$, and define v_γ on $E(\bar{a})$ as in the previous step. We let S be the set of $\gamma \in \mathcal{R}$ such that the valuation v_γ on $E(\bar{a})$ ramifies in L.

Step 7. If $\gamma \in \mathcal{R}$, then there is an open ball B containing γ and such that $B \subset S$ if $\gamma \in S$, and $B \cap S = \emptyset$ if $\gamma \notin S$.

Observe that because the residue field of $(E(\bar{a}),v_\gamma)$ is algebraically closed, if the valuation v_γ does not ramify in L, then the extension $L/E(\bar{a})$ is immediate. There is a formula $\theta(\bar{x})$ (with parameters in E) of the language of valued fields, such that $(E(\bar{a}),v_\gamma) \models \theta(\bar{a})$ if and only if v_γ ramifies in L.

The reasoning done in Step 5 tells us that given a formula $\theta(\bar{x})$ of the language of valued fields with parameters in E, and some $\gamma \in \mathcal{R}$ such that $(E(\bar{a}),v_\gamma) \models \theta(\bar{a})$, there is an open ball B containing γ and such that for any $\delta \in B$, $(E(\bar{a}),v_\delta) \models \theta(\bar{x})$.

Putting these two observations together proves step 7.

Step 8. $\sigma(S) \subseteq S$.

Observe that by step 3, and because $[L : E(\bar{a})]/e$ is a power of p, the index of ramification of v_γ in L will be a power of p.

Let $\gamma \in S$, and fix an extension v of v_γ to $L(\sigma(\bar{a}))$. Then the isomorphism σ^{-1} sends $(E(\sigma(\bar{a})), v)$ to $(E(\bar{a}), v_{\sigma(\gamma)})$, and therefore it suffices to show that the restriction of v to $\sigma(L)$ ramifies over $E(\sigma(\bar{a}))$.

We also know that $L\sigma(\bar{a}) = \sigma(L)(\bar{a})$, and that L and $E(\bar{a}, \sigma(\bar{a}))$ are linearly disjoint over $E(\bar{a})$, $\sigma(L)$ and $E(\bar{a}, \sigma(\bar{a}))$ are linearly disjoint over $E(\sigma(\bar{a}))$. If $\Gamma = \langle\gamma\rangle \otimes \mathbb{Z}[1/d_n]$, then $v(E(\bar{a}, \sigma(\bar{a})) \subset \Gamma$, but $v(L) \not\subset \Gamma$ because p does not divide d_n. If $\sigma(L)/E(\sigma(\bar{a}))$ is not ramified for the valuation v, then it is immediate, with value group contained in Γ. As $(E(\bar{a}, \sigma(\bar{a}))$ is a totally ramified extension of $E(\sigma(\bar{a}))$, it follows that the value group of $\sigma(L)(\bar{a})$ is contained in Γ. This contradicts $\sigma(L)(\bar{a}) = L(\sigma(\bar{a}))$.

Step 9. Embedding $E(a)_\sigma$ into $E((t^{\mathbb{R}}))$.

Note that if $\gamma \in S$ and $0 \neq r \in \mathbb{R}$, then $r\gamma \in S$: this is because the valuations v_γ and $v_{r\gamma}$ are equivalent. If $n > 1$, by steps 7 and 8, the conclusion of Lemma (3.14) holds. Hence there is some $\gamma \in S$ such that if B is any open ball containing γ, then there are infinitely many $k \in \mathbb{N}$ such that $\frac{\|\gamma\|}{\|\sigma^k(\gamma)\|}\sigma^k(\gamma) \in B$. Note that this is trivially true if $n = 1$.

Fix such a γ. For $i = 0, \ldots, n-1$, we identify $\sigma^i(a)$ with t^{γ_i}. By induction, using the fact that for $m > 0$, the equation $\prod_{i=0}^{n} \sigma^{i+m}(a_i^{d_i})$ determines $\sigma^{n+m}(a)$ up to possibly multiplication by a d_n-th root of 1, and using the fact that a is a generic of the connected group B, it follows that we may identify $\sigma^i(a)$ with t^{γ_i} for all $i \geq 0$. Extend this embedding to L. We therefore view $L(\sigma^i(a) \mid i \geq 0)$ as a valued subfield of $E((t^{\mathbb{R}}))$, the value group of $E(\sigma^i(a) \mid i \geq 0)$ being contained in $\Gamma = \langle\gamma\rangle \otimes \mathbb{Z}[1/d_n]$.

Step 10. The final contradiction.

By step 3, because $[L : E(\bar{a})]/e$ is a power of p, and $(e, p) = 1$, we know that the index of ramification of $v = v_\gamma$ in L is a power of p. Moreover, because E is algebraically closed, the decomposition subfield and inertia subfield of v in L coincide, and L is obtained from this inertia subfield by a tower of Artin-Schreier extensions. Hence there are $b, c \in L$ with $c^p - c = b$, such that the restriction of v to $E(\bar{a}, c)$ ramifies over $E(\bar{a})$, but its restriction to $E(\bar{a}, b)$ does not.

By Proposition (3.11) applied to Γ, $b_{|0}$ is a polynomial in $\bar{a}, \bar{a}^{-1}$, and we may assume that $b_{|0} = \sum_{\nu \in J} c_\nu \bar{a}^\nu$, where ν ranges over a finite subset J of $\Gamma \setminus p\Gamma$, and the c_ν are in E. Let $P(\bar{a}, T)$ be the minimal polynomial of b over $E(\bar{a})$. Then, by Proposition (3.11) again, there is some $Q(\bar{a}) \in E[\bar{a}, \bar{a}^{-1}]$ such that $v(b - Q(\bar{a})) > 0$, and $v(P(Q(\bar{a}))) > \sup\{0, 2v(P'(Q(\bar{a})))\}$.

Consider the following formula $\varphi(\bar{x})$ (with parameters in E):

$$v(P(Q(\bar{x}))) > \sup\{0, 2v(P'(Q(\bar{x})))\} \wedge v(Q(\bar{x}) - \sum_{\nu \in J} c_\nu \bar{x}^\nu) > 0.$$

Then $(E(\bar{a}), v_\gamma) \models \varphi(\bar{a})$. Let B be an open ball containing γ and such that if $\delta \in B$, then $(E(\bar{a}), v_\delta) \models \varphi(\bar{a}))$. Let $k \in \mathbb{N}$ be such that $\sigma^k(\gamma) \in B$. Then $(E(\bar{a}), v_{\sigma^k(\gamma)}) \models \varphi(\bar{a})$. We saw that σ^k defines an isomorphism of valued fields between $(E(\bar{a}), v_{\sigma^k(\gamma)})$ and $(E(\sigma^k(\bar{a})), v)$. Hence $(E(\sigma^k(\bar{a})), v) \models \varphi^k(\sigma^k(\bar{a}))$, where φ^k is obtained from φ by applying σ^k to the parameters from E. We let b_k be a root of $P^{\sigma^k}(\sigma^k(\bar{a}), T)$ satisfying $v(b_k - \sum_{\nu \in J} \sigma^k(c_\nu \bar{a}^\nu)) > 0$, and c_k a solution of $T^p - T = b_k$.

We let I be the set of positive integers k such that $\sigma^k(\gamma) \in B$. We will shrink I successively.

Each b_k is a field conjugate of $\sigma^k(b)$, and it therefore follows that there is an infinite subset I_1 of I such that if $k < \ell \in I_1$ then $\sigma^{\ell-k}(b_k) = b_\ell$. By Step 1, this implies that $E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))(b_k) = E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))(b_\ell)$, and therefore $E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))(c_k) = E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))(c_\ell)$. The theory of Artin-Schreier extensions tells us that there is a non-zero $c(k,\ell) \in \mathbb{F}_p$ and $g \in E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))$ such that $b_k - c(k,\ell)b_\ell = g^p - g$ for some $g \in E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))$. Thus, there is an infinite subset I_2 of I_1 such that if $k < \ell \in I_2$, then $c(k,\ell) = 1$.

Let $D = \{\nu \cdot \gamma \mid \nu \in J\}$ $(= \mathrm{Supp}(b) \cap (-\infty, 0)$; we use the inner product notation $\nu \cdot \gamma$ for $\sum_{i=0}^{n-1} \nu_i \gamma_i)$. Then $\mathrm{Supp}(b_k) \cap (-\infty, 0) = \sigma^k(D)$, no element of $\sigma^k(D)$ is divisible by p in $\langle \sigma^k(\gamma) \rangle$, and similarly for $\mathrm{Supp}(b_\ell)$. Then $\sum_{\nu \in J} \sigma^k(c_\nu \bar{a}) - \sigma^\ell(c_\nu \bar{a}) = g_1^p - g_1$ for some $g_1 \in E(\sigma^k(\bar{a}), \ldots, \sigma^\ell(\bar{a}))$ with support contained in $(-\infty, 0)$.

Observe that because $\gamma_0, \ldots, \gamma_{n-1}$ are $\mathbb{Q}$-linearly independent, $\nu \neq \nu'$ implies $\nu \cdot \gamma \neq \nu' \cdot \gamma$. Hence, there is a unique permutation $f = f_{k,\ell}$ of J such that $\nu \cdot \sigma^k(\gamma)$ and $f(\nu) \cdot \sigma^\ell(\gamma)$ are proportional for all $\nu \in J$, the coefficient of proportionality $\lambda = \lambda(\nu, k, \ell)$ being a power of p.

Hence, there is an infinite subset I_3 of I_2 such that if $k < \ell \in I_3$ then $f_{k,\ell} = id$. Fix $\nu = (\nu_0, \ldots, \nu_{n-1}) \in J$, $k < \ell$ in I_3. Recall that the elements of γ form a basis of the free $\mathbb{Z}[1/d_n]$-module Γ. Hence, the existence of $m \in \mathbb{Z}$ such that $\nu \cdot \sigma^k(\gamma) = p^m \nu \cdot \sigma^\ell(\gamma)$ translates into the following: if $u = \sum_{i=0}^{n-1} \nu_i \gamma_i$, then $A^k(u) = p^m A^\ell(u)$. So, $A^{k-\ell}$ has an eigenvalue which is a power of p. This contradicts our assumption on B, and finishes the proof.

(4.6) [thm1]**Theorem**. Let Ω be a model of ACFA, let G be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let B be a definable modular subgroup of $G(\Omega)$.

(1) Then B is stable and stably embedded.
(2) Every definable subset of B^n is a Boolean combination of translates of definable subgroups of B^n. The definable subgroups of B^n are defined over E.
(3) If $a \in B$ and $F = \mathrm{acl}_\sigma(F)$ contains E, and L is a finite σ-stable extension of $F(a)_\sigma$, then L is contained in $F(b)_\sigma$ for some b and N with $[N]b = a$.

Proof. We have shown (3) when $\mathrm{evSU}(B) = 1$ in Propositions (4.1) and (4.5). By Lemmas (1.3) and (3.7), this implies that if $a \in B$, then $tp(a/E)[m]$ is stationary for every $m \geq 1$. Hence, if $\mathrm{evSU}(B) = 1$, then (1) holds by (1.4).

Let us now assume that $\mathrm{evSU}(B) > 1$. Replacing B by $p_n(B)$ for some n, we may assume that if $a \in B$, then $\sigma(a) \in E(a)^{alg}$. Let m be large enough so that if a is a generic of B over E, then $SU(a/E)[m] = \mathrm{evSU}(a/E) = k$, and replace B by $B(m)$ which is the connected component of the σ^m-closure of B. We now work in (Ω, σ^m). Using the modularity of $B(m)$ (see (1.4)), there is a sequence $(0) = B_0 \subset B_1 \subset \cdots \subset B_k = B(m)$ of subgroups of $B(m)$, with $[B_i : B_{i-1}] = \infty$ for $i = 1, \ldots, k$ [Take a sequence $F_{k-1} \subset \cdots \subset F_1$ of difference subfields of $\Omega[m]$ such that $SU(a/F_i)[m] = i$. Then for each i, a is the generic of a coset of a σ^m-closed subgroup B_i of G of $SU[m]$-rank i, by Theorem (1.5).] Then $\mathrm{evSU}(B_i/B_{i-1}) = 1$ for $i = 1, \ldots, k$, and by Proposition (1.6) $B(m)$ is stable, stably embedded. Note that this result holds for every $B(m\ell)$ where $\ell \geq 1$. This implies that for every $E \subset F_1 = acl_{\sigma^{m\ell}}(F_1) \subset F_2 = acl_{\sigma^{m\ell}}(F_2)$ and $b \in B(m\ell)$, $tp(b/F_1)[m\ell]$ is definable

over F_1 and therefore has a unique non-forking extension to F_2. Hence, $F_2(F_1(b)^{alg})$ has no finite $\sigma^{m\ell}$-stable extension (see Lemma (1.3)). Thus for every $E \subset F_1 = \mathrm{acl}_\sigma(F_1) \subset F_2 = \mathrm{acl}_\sigma(F_2)$ and $b \in B$, $F_2(F_1(b)^{alg})$ has no finite σ-stable extension. This implies that every extension over an algebraically closed set of the generic type of B is definable and stationary. Hence every type realised in B is stable and stably embedded. This shows (1).

In particular every definable subset of B^n is a Boolean combination of translates of definable subgroups of B^n, since B with the induced structure is stable and modular, whence weakly normal by [HP].

(3) Let $F = \mathrm{acl}_\sigma(F)$ contain E, and let $a \in B$. Let C be the σ-closed connected subgroup of B such that a is a generic of the coset $a + C$ over F. Let $a_1 \in a + C$ be independent from a over F. Then $tp(a/Fa_1)$ is completely determined by the class of $(a - a_1)$ in C/C^*, where $C^* = \bigcap_{n\geq 1}[n]C$. This comes from the fact that $tp(a/Fa_1)$ is uniquely determined by the set of cosets of definable subgroups D of C which are defined over $F(a_1)$ and which contain $(a - a_1)$; as $(a - a_1)$ is a generic of C over $F(a_1)_\sigma$, these subgroups D must have finite index in C, and therefore be contained in $[n]C$ for some n. For each n choose $b_n \in G$ such that $[n]b_n = a - a_1$, and let $F_1 = \mathrm{acl}_\sigma(Fa_1)$. Then $tp(a/F_1)$ is completely determined by $qftp(a, b_2, \ldots, b_n, \ldots/F_1)$. Similarly, for every $m \geq 1$, $tp(a/F_1)[m]$ is completely determined by $qftp(a, b_2, \ldots, b_n, \ldots/F_1)[m]$. That is (see (1.3)), the field $F_1(a, b_2, \ldots)_\sigma$ has no finite proper σ-stable extension.

Let L be a finite σ-stable extension of $F(a)_\sigma$. Then $LF_1(a, b_2, \ldots)_\sigma$ is a finite σ-stable extension of $F_1(a, b_2, \ldots)_\sigma$, so that $L \subset F_1(b_n)_\sigma$ for some n.

Note that F_1 contains a root of $[n]x = a_1$. Hence $F_1(b_n)_\sigma = F_1(c_n)_\sigma$ where $[n]c_n = a$, and $L \subset F_1(c_n)_\sigma$. As a_1 was independent from a over F, this implies that $L \subset F(c_n)_\sigma$.

(4.7) **Some remarks about** $B/[n]B$**.** Let A be a semi-abelian variety defined over $E = \mathrm{acl}_\sigma(E)$, and let $B \subset A(\Omega)$ be a definable modular subgroup of $A(\Omega)$, n an integer bigger than 1. Then B has finite index in $\mathrm{Ker}(f)$ for some $f \in \mathrm{End}_\sigma(A)$, and we will assume that $B = \mathrm{Ker}(f)$. Since Ω is elementarily equivalent to an ultraproduct of difference fields $(\mathbb{F}_p^{alg}, \mathrm{Frob}_q)$ (see [H2]), we know that $[B : [n]B] = |B \cap A[n]|$. Consider $A[n]/f(A[n])$. Then $[A[n] : f(A[n])] = |\mathrm{Ker}(f) \cap A[n]| = |B \cap A[n]|$. Define

$$\varphi : B \to A[n]/f(A[n])$$

as follows: if $a \in B$ take $b \in A$ such that $[n]b = a$, and define $\varphi(a) = f(b) + f(A[n])$. Since distinct choices of b differ by an element of $A[n]$, this map is well-defined. One checks easily that it is a group homomorphism, and that its kernel is precisely $[n]B$, so that it is an isomorphism.

In general, a subgroup of $A(\Omega)$ of the form $\mathrm{Ker}(f)$ for some $f \in \mathrm{End}_\sigma(A)$ is not connected, and so this result is not entirely satisfactory - how does one recognise $B^0/[n]B$? One can do this in a slightly different manner. Replacing $B = \tilde{B}^0$ by $p_N(B)$ for some N and A by $B_{(N)}$ we may assume that $B = \tilde{B}_{(1)}$, and that B is Zariski dense in A. If we define C_1, C_2 by

$$C_1 \times \{0\} = B_{(1)} \cap (A \times \{0\}), \qquad \{0\} \times C_2 = B_{(1)} \cap (\{0\} \times A^\sigma),$$

the group $B_{(1)}/C_1 \times C_2$ is the graph of a (definable in ACF) group isomorphism

$$f : A/C_1 \to A^\sigma/C_2.$$

If $h_1 : A \to A/C_1$ and $h_2 : A^\sigma \to C_2$ are the natural isogenies, $a \in B$ if and only if $fh_1(a) = h_2(\sigma(a))$.

Let $A' = A^\sigma/C_2$, let $F : A \to A'$ be defined by $F(x) = fh_1(x) - h_2(\sigma(x))$. Then $B = \mathrm{Ker}(F)$. Define $\varphi : B \to A'[n]/F(A[n])$ as follows: if $a \in B$, let $b \in A$ be such that $[n]b = a$, and set $\varphi(a) = F(b) + F(A[n])$. As A and A' are isogenous, we know that $[A'[n] : F(A[n])] = |\mathrm{Ker}(F) \cap A[n]| = |B \cap A[n]|$, and we get an isomorphism.

(4.8) **Problem**. In positive characteristic, do there exist any stable definable subgroups of $\mathbb{G}_a$?

Bibliography

[CH] Z. Chatzidakis, E. Hrushovski, Model theory of difference fields, Trans. Amer. Math. Soc. 351 (1999), pp. 2997-3071.

[CHP] Z. Chatzidakis, E. Hrushovski, Y. Peterzil, Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics, Proceedings of the London Math. Society (3) 85 (2002), 257 – 311.

[C] R.M. Cohn, Difference algebra, Tracts in Mathematics 17, Interscience Pub. 1965.

[D] F. Delon, Hensel fields in equal characteristic $p > 0$, in: *Model Theory of Algebra and Arithmetic, Proc. Karpacz 1979*, Lecture Notes in Mathematics Nr 834, Springer-Verlag Berlin Heidelberg 1980.

[H] E. Hrushovski, The Manin-Mumford conjecture and the model theory of difference fields, Ann. Pure Appl. Logic 112 (2001), no. 1, 43 – 115.

[H2] E. Hrushovski, The first-order theory of the Frobenius, preprint (1996).

[HP] E. Hrushovski, A. Pillay, Weakly normal groups, in: Logic Colloquium 85, North Holland 1987, 233 – 244.

[HP2] E. Hrushovski, A. Pillay, Groups definable in local fields and pseudo-finite fields, Israel J. of Math. 85 (1994), 203 –262.

[KP] P. Kowalski, A. Pillay, A note on groups definable in difference fields, Proceedings AMS, 130, (2001), 205-212.

[LS] S. Lang, J.-P. Serre, Sur les revêtements non ramifiés des variétés algébriques. (French) Amer. J. Math. 79 (1957), 319 – 330. Erratum in: Amer. J. Math. 81 (1959) 279 – 280.

[R] A. Robinson, *Complete theories*, North-Holland, Amsterdam 1956.

[S] O.F.G. Schilling, The theory of valuations, AMS Mathematical Survey 4, New York 1950.

[Se] J. -P. Serre, Topics in Galois Theory, Research Notes in Mathematics Vol. 1, Jones and Bartlett Pub., Boston 1992.

[W] V. Weispfenning, Quantifier elimination and decision procedures for valued fields. Models and sets (Aachen, 1983), Lecture Notes in Math., 1103, Springer, Berlin, 1984, 419 — 472.

Current addresses:

UFR de Mathématiques
Université Paris 7 - Case 7012

75205 Paris Cedex 13
France
e-mail: zoe@logique.jussieu.fr

Institute of Mathematics
The Hebrew University
Givat Ram
91904 Jerusalem
Israel
e-mail: ehud@math.huji.ac.il